Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería de Sistemas e Informática

Escuela Académico Profesional de Ingeniería de Sistemas

Integración de accesos en servicio de directorio de una entidad bancaria, usando ingeniería de roles y perfiles

TESINA

Para optar el Título Profesional de Ingeniero de Sistemas

AUTOR

Huber Zósimo LLANCA MORALES

ASESOR

Winston Ignacio UGAZ CACHAY

Lima, Perú

2016

Referencia bibliográfica

Llanca, H. (2016). *Integración de accesos en servicio de directorio de una entidad bancaria, usando ingeniería de roles y perfiles*. [Tesina de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Escuela Académico Profesional de Ingeniería de Sistemas]. Repositorio institucional Cybertesis UNMSM.

DEDICATORIA:

Dedicado a Dios mi fortaleza que siempre está conmigo y a mi señora madre por su ejemplo y dedicación.

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

"Universidad del Perú, Decana de América"

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS

INTEGRACIÓN DE ACCESOS EN SERVICIO DE DIRECTORIO DE UNA ENTIDAD BANCARIA, USANDO INGENIERÍA DE ROLES Y PERFILES

Autor: LLANCA MORALES, Huber Zósimo

Asesor: UGAZ CACHAY, Winston Ignacio

Título: Tesina, para optar el Título Profesional de Ingeniero de Sistemas

Fecha: Jun 2016

RESUMEN

Hoy en día el proceso de gestión de perfiles y accesos es un factor muy importante para una organización pues como sabemos este provee de recursos y servicios de TI a los colaboradores para el desempeño de sus funciones, la automatización del proceso de entrega de accesos y una correcta segregación de accesos nos asegura que se cumplan los pilares de las seguridad de la información que son confidencialidad, integridad y disponibilidad, esto es muy fundamental pues la empresa donde se va implementar es una entidad bancaria del país que está regulada por la SBS Superintendencia de Banca y Seguros del Perú e internacionalmente por SOX (Ley Sarbanes-Oxley).

Palabra claves: Servicio de Directorio, Perfiles, Grupos de Seguridad y Active Directory.

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

"Universidad del Perú, Decana de América"

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS

INTEGRATION OF ACCESS IN SERVICE DIRECTORY OF A BANK USING ENGINEERING ROLES AND PROFILES

Autor: LLANCA MORALES, Huber Zósimo

Asesor: UGAZ CACHAY, Winston Ignacio

Title: Thesis to choose the Professional Title Systems Engineer

Date: Jun 2016

ABSTRACT

Today the management process profiles and access is a very important factor for an organization because as we know this provides resources and IT services to employees to perform their functions, automation of the delivery process of access and proper segregation of hits assures us that the pillars of information security are confidentiality, integrity and availability are met, this is very important because the company which will implement a bank in the country is regulated by the SBS Superintendency banking and Insurance of Perú and internationally for SOX (Sarbanes-Oxley).

Key word: Directory Service, Profiles, Security Groups and Active Directory.

ÍNDICE

Tabla de Ilustraciones

Capítulo 1: PLANTEAMIENTO METODOLÓGICO

1.1 ANTECEDENTES

Actualmente en la entidad bancaria existe la necesidad de cumplir con los criterios de Seguridad de la Información como son confidencialidad, integridad y disponibilidad, pero para ello debe contar con aplicaciones que aseguren una eficiente entrega de los accesos, una de las principales aplicaciones que nos podría ayudar a este cumplimiento es el Servicio de Directorio de la empresa, pero este no se encuentra correctamente organizado, no tiene definida una estructura de grupos que integre los servicios más básicos como son correos corporativos, directorios compartidos, dispositivos de almacenamientos, intranet y niveles de internet. Por ello el Proceso de entrega de acceso se torna lento y poco eficiente ya que el equipo de Soporte Usuarios tiene que asignar cada uno de estos recursos por cada usuario lo que genera demoras en la atención y el incumplimiento de sus SLAS que son en promedio 4 hras por la atención de un recurso o servicio, inclusive en las altas de usuarios se dan casos que el colaborador ya está laborando y no cuenta con estos recursos básicos, lo mismo sucede en los movimientos de accesos cuando los colaboradores cambian de puesto y se tiene que reasignar nuevamente estos servicios. Todo esto lo vemos reflejado en los monitoreos periódicos que realiza el área de Seguridad de Información donde se encuentran casos de colaboradores que cambiaron de puesto pero aún conservan accesos anteriores, en varias oportunidades ya ha sido materia de observación de auditoría que ha observado muchos casos de usuarios con accesos no autorizados, cabe señalar que los monitoreos que se realizan son muy complejos pues no existe mucha trazabilidad en la estructura de accesos del Directorio Activo.

También surge los problemas de carga operativa para la unidad de Soporte Usuarios quienes otorgan los accesos a los usuarios, ellos han manifestado que les falta personal para otorgar de manera eficiente los recursos (servicios de correos, directorios compartidos, dispositivos de almacenamientos, Intranet y niveles de internet) y están seguros que con más personal podrán, la empresa se ha negado a contratar más personal por falta de presupuesto.

Otra problemática importante que se evidencia son los accesos no autorizados de los usuarios que difieren con los señalado en las políticas de seguridad de accesos que señala que los niveles de accesos se deben otorgar de acuerdo a los roles que desempeña cada cargo de la organización teniendo en cuenta las divisiones, áreas y jerarquías todo ello plasmado en una serie de matrices de perfiles con cargos autorizados a recursos y aplicaciones, es necesario encontrar una solución pues se trata de una entidad bancaria que maneja información confidencial de usuarios internos y de clientes.

1.2 FORMULACIÓN DEL PROBLEMA

¿El uso de roles y perfiles reduce el tiempo de entrega de accesos a recursos y servicios TI a los usuarios de una organización?

1.3 IMPORTANCIA (JUSTIFICACIÓN)

- El cumplimiento de la circular G-140-2009 emitida por la Superintendencia de Banca y Seguros *("Articulo 5; 5.1 Seguridad Lógica, a) Procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios."*) que toma como referencia estándares internacionales como el ISO 17799 e ISO 27001.

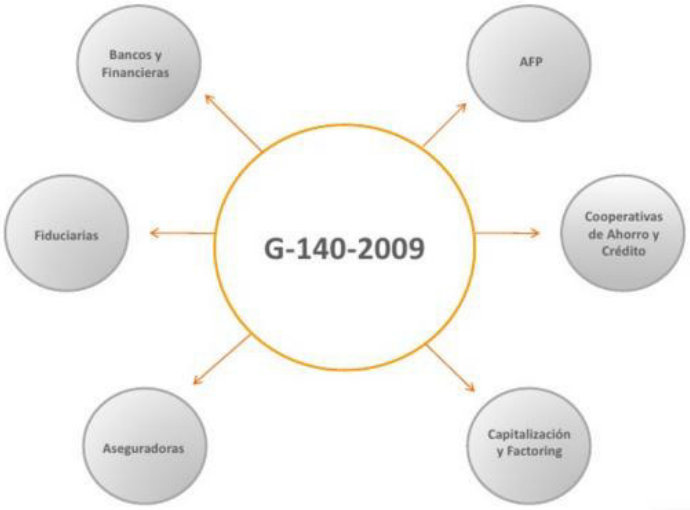


Ilustración 1: Entidades asociadas al Cumplimiento de la G-140-2009

Fuente: http://es.slideshare.net/ArandaSoftware/cumplimiento-circular-g1402009per

- La importancia de automatizar un proceso de entrega de accesos a colaboradores de una organización que provee eficientemente los servicios y recursos para que estos puedan desempeñar sus funciones.
- La minimización de la carga operativa que pueda tener el área encargada de la habilitación de accesos, lo que implica un ahorro en tiempo horas hombre.
- La segregación de accesos que es una de las principales actividades de control interno destinada a prevenir o reducir el riesgo de errores o irregularidades en accesos no autorizados.

1.4 OBJETIVOS

1.4.1 *Objetivo General*

Diseñar una Estructura de Grupos de Seguridad en el Servicio de Directorio de la Entidad Bancaria, que automatice y mejore los tiempos de atención de accesos a los servicios y recursos TI, usando Ingeniería de Roles y Perfiles.

1.4.2 *Objetivos Específicos*

- Mejorar los tiempos de atención de requerimientos de accesos de los recursos de TI integrados al Servicio de Directorio.
- Diseñar una estructura de grupos de seguridad para los diversos puestos estableciendo niveles de jerarquías e integrar los Servicios de TI a los grupos de seguridad asociando usuarios a cada grupo según su cargo.
- Elaborar matrices de perfiles de accesos que se otorgan en el Servicio de Directorio, asegurando la trazabilidad de los accesos a recursos TI asociados a los cargos de la organización.
- Establecer mejoras en el cumplimiento de la Circular G-140-2009 emitida por SBS (Superintendencia de Banca y Seguros) y los criterios de Seguridad de la Información (confidencialidad, integridad y disponibilidad) en los permisos otorgados a los colaboradores por medio del Servicio de Directorio.

1.5 ALCANCES

- La organización que será beneficiada con este proyecto de tesina es una entidad bancaria que promueve principalmente el desarrollo económico de las pymes, cuenta con oficinas principales y sucursales de agencias.
- Se realizará un análisis de como realiza la Entidad Bancaria la entrega de accesos que se pueden integrar en el Servicio de Directorio y como están segregados los mismos.
- Se va desarrollar una estructura de grupos de seguridad asociada a todas las unidades organizativas de la empresa como son: División, Gerencias, Áreas y Cargos de Colaboradores.
- Se integraran una serie de políticas asociados a Servicios de Directorio como son correos, directorios compartidos, dispositivos de almacenamiento y niveles de internet, todo ello con un enfoque de ingeniería de roles y perfiles.
- La implementación de la solución será aplicable en todas las unidades organizativas que existen en las oficinas principales y sucursales del banco, además es aplicable en cualquier organización que cuente con una estructura organizativa con niveles de jerarquía.

Capítulo 2: MARCO TEÓRICO

2.1 SERVICIO DE DIRECTORIO (SD)

2.1.1 CONCEPTO DE SERVICIO DE DIRECTORIO

Es una aplicación de software especializada que administra información sobre los recursos disponibles en una red donde acceden los usuarios, permite a los administradores gestionar los accesos de usuarios a los recursos y servicios de dicha red. El elemento fundamental del SD es el *directorio* que es un elemento que almacena información sobre los distintos recursos de red. Existen muchos estándares de servicios de directorios siendo el más conocido el X500.

2.1.2 FUNCIONES DE UN SERVICIO DE DIRECTORIO

Entre la funciones que se pueden establecer en los servicios de directorio tenemos los siguientes:

- **Encontrar Información**: Los directorios electrónicos permite acceder a la información contenida de manera más eficiente a lo tradicional.
- **Gestionar Información:** Accesibilidad desde todas las aplicaciones que están sincronizadas y pueden acceder de diferentes maneras a los datos contenidos.
- **Aplicación de la Seguridad:** Gestión de Claves públicas y certificados digitales .[1]

2.1.3 ACTIVE DIRECTORY

Active Directory es el Servicio de Directorio de Microsoft que permite centralizar, estructurar, organizar y controlar los recursos de red en los entornos Windows.Se trata de un directorio centralizado (una base de datos), que contiene los objetos de

[1] *Introducción al Servicio de Directorios; Rafael Calzada Prada*

red y que permite a los usuarios localizar, gestionar y explotar fácilmente los recursos.[2]

2.1.3.1 CARACTERISTICAS DEL ACTIVE DIRECTORY

El Active Directory es un servicio que el directorio proporciona una serie de diferentes servicios en relación con el almacenamiento organizado de recursos de red. Los siguientes puntos ponen de relieve algunas de las características del Active Directory:

- **Escalabilidad:** Puede crecer y soportar un elevado número de objetos.
- **Integración con el DNS:** Los nombres de dominio son nombres DNS y tienen que estar registrados en él**,** es necesario instalar DNS antes de poder instalar AD.
- **Extensible:** Permite personalizar las clases y objetos que están definidas dentro de AD según las necesidades propias.
- **Seguridad:** Incorpora las características de seguridad de la versión Windows Server 2008 y se puede controlar el acceso a cada objeto.
- **Multimaestro:** No distingue entre controladores de dominios primarios o secundarios, cualquier controlador de dominio puede procesar cambios del directorio.
- **Flexible:** Permite reflejar la organización lógica y física de la empresa u organización sigue el estándar LDAP (Lightweight Directory Access Protocol).

2.1.3.2 ELEMENTOS DEL ACTIVE DIRECTORY

DOMINIO

Colección de equipos que comparten la base de datos del Active Directory y que se administran de forma conjunta. Los controladores de dominio, almacenan una copia de la base de datos y permiten gestionarla y administrarla. También controlan el acceso a la red, a la BD del directorio y a los recursos compartidos.

Características

[2] BRAHIM NEDJIMI, LOIC THOBOIS; "Preparación a la certificación MCSE Exchange Server 2013" Editorial: ENI (2014); Barcelona-España, Pág. 34.

- El dominio es la unidad central de la estructura lógica de AD.
- Un dominio se crea al generar el primer controlador del dominio.
- Mantiene su ACL (lista de control de acceso) con todos los permisos para los recursos del dominio, controlando los usuarios que pueden acceder al mismo y el tipo de acceso
- Los elementos de la base de datos del directorio (cuentas de usuarios, grupos, equipos y recursos compartidos, como impresoras y carpetas) los usarán todos los equipos del dominio.
- Todos los recursos (u objetos) de la red existen en un dominio y cada dominio almacena información exclusivamente de los objetos que contiene.

OBJETOS

Representan un recursos de la red, lo objetos principales son los siguientes:

Unidades Organizativas (OU, Organizatial Units)

Los recursos del dominio se organizan en Unidades Organizativas (OU, Organizational Units), que son contenedores (como directorios) que permiten ordenar los recursos u objetos dentro de un dominio.

Características

- Contienen agrupaciones lógicas de recursos, como archivos, impresoras, cuentas, aplicaciones y otros recursos del dominio.
- Son como subgrupos dentro del dominio que reflejan, normalmente, la estructura funcional o de negocios de una organización.
- Sólo pueden contener objetos del dominio al que están asociados
- Crean vistas del directorio más pequeñas y manejables.

Se puede delegar la autoridad sobre las mismas, para manejar con más facilidad el acceso a los recursos administrativos.

Grupos

Es el conjunto de objetos del mismo tipo, de modo que se trata como si el conjunto fuera uno solo. Se utiliza fundamentalmente para asignar derechos a accesos a recursos, estos objetos simplifican bastante las tareas.

Usuarios

Son aquellos que tienen cuentas que le permiten identificarse en el sistema y poder tener accesos a los recursos y servicios, las cuentas son únicas.

Equipos

Es el conjunto de ordenadores que componen una red y forman parte de un dominio, desde el dominio se puede administrar cada uno de los equipos.

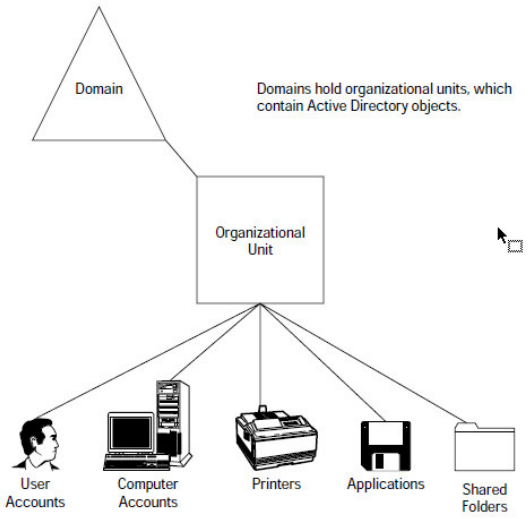


Ilustración 2: Estructura Lógica AD

Fuente : CURT SIMMONS; Active Directory Bible; Pág. 7

2.1.3.3 GRUPOS DE SEGURIDAD Y DISTRIBUCIÓN

Según los conceptos que indica Microsoft existen dos tipos de grupos en Active Directory: grupos de distribución y grupos de seguridad. Los grupos de distribución se utilizan para crear listas de distribución de correo electrónico y los grupos de seguridad para asignar permisos a los recursos compartidos en red.

GRUPOS DE DISTRIBUCIÓN

Los grupos de distribución sólo se pueden utilizar con aplicaciones de correo electrónico (como Exchange) para enviar correo electrónico a grupos de usuarios.

Los grupos de distribución no tienen habilitada la seguridad, lo que significa que no se pueden incluir en las listas de control de acceso discrecional (DACL).

GRUPOS DE SEGURIDAD

Si se utilizan adecuadamente, los grupos de seguridad suponen un modo eficaz de asignar el acceso a los recursos de su red. Los grupos de seguridad permiten:

- **Asignar derechos de usuario a grupos de seguridad en Active Directory :** Los derechos de usuario se asignan a los grupos de seguridad para determinar qué acciones pueden llevar a cabo los miembros del grupo en el ámbito de un dominio (o bosque). Con la directiva de grupo, puede asignar derechos de usuario a los grupos de seguridad, lo que le ayudará a delegar tareas específicas.
- **Asignar permisos a grupos de seguridad en recursos :** Los permisos no se deben confundir con los derechos de usuario. Los permisos se asignan al grupo de seguridad en el recurso compartido. Los permisos determinan qué usuarios pueden tener acceso al recurso y el nivel de acceso, como control total.
- **Convertir grupos de seguridad en grupos de distribución y viceversa:** Un grupo de seguridad puede convertirse en un grupo de distribución y viceversa en cualquier momento, pero sólo si el nivel funcional de dominio está establecido en Windows 2000 nativo o posterior.[3]

2.1.3.4 DIRECTIVAS DE GRUPO DE ACTIVE DIRECTORY

Un razón principal para implementar Active Directory son las políticas o directivas de grupo que este posee, la directiva de grupo es una infraestructura que le permite implementar configuraciones específicas para los usuarios y equipos. Las configuraciones de la directiva de grupo se encuentran en los objetos de directiva de grupo (GPO), que se vinculan con los siguientes contenedores de servicio de directorio de Active Directory: sitios, dominios o unidades organizativas (OU).

[3] https://msdn.microsoft.com/es-es/library/cc781446(v=ws.10).aspx

Luego, los destinos afectados evalúan las configuraciones dentro de las GPO mediante la naturaleza jerárquica de Active Directory. [4]

Objetos de Directiva de Grupo (GPO)

Los GPO contienen configuraciones de directivas y pueden verse como un documento de directiva que aplica opciones de configuración a los equipos y a los usuarios sobre los que ejerce control.

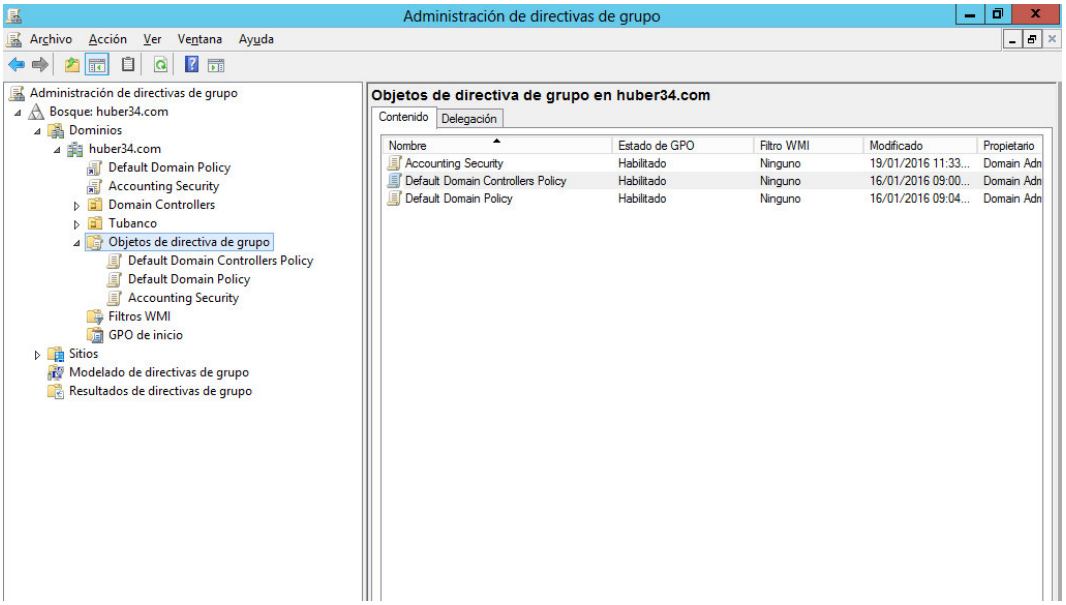


Ilustración 3: Objetos de Directiva de Grupo

Fuente: Creación Propia

En el Administrador de Directivas de grupos se pueden apreciar 3 GPOs predeterminados al dominio huber34.com ellos son:

Accounting Security (Seguridad de cuentas). Se trata de un GPO personalizado creado específicamente para el dominio en mención.

Default Domain Controller Policy (Directiva predeterminada de controladores de dominio). La instalación del rol de servidor AD DS crea esta directiva de forma predeterminada. Contiene opciones de configuración de directiva que se aplican específicamente a controladores de dominio.

[4] *https://technet.microsoft.com/es-es/windowsserver/bb310732.aspx*

Default Domain Policy (Directiva predeterminada de dominios). La instalación del rol de servidor AD DS crea esta directiva de forma predeterminada. Contiene las opciones de configuración de directiva que se aplican a todos los equipos y usuarios del dominio.[5]

Herencia de Directivas de Grupo

Es una característica que tienen las GPOs cuyas políticas se pueden replicar a todos los equipos y usuarios de un dominio o OU en particular, por ejemplo si se crea un GPO Bloqueo de puerto USB y esto se asocia a un Dominio, esto aplicará a todas las OU que pertenecen a dicho dominio restringiendo el accesos a todos los usuarios.

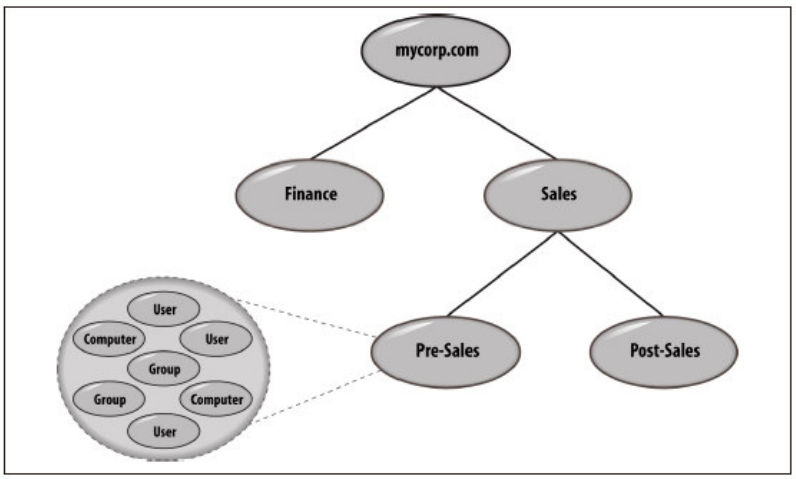


Figure 2-1. A hierarchy of objects

Ilustración 4: Herencia de Objetos

Fuente: Libro Active Directory; Brian Desmond, Joe Richards, Robbie Allen y Alistar g. Lowe Norris; Pág. 6

2.2 ADMINISTRACIÓN DE PERFILES Y ACCESOS

En el presente las Organizaciones consideran un factor muy importante a la Administración de Perfiles y Accesos pues este provee de recursos y servicios tecnológicos a los colaboradores que laboran en ella.

[5] *https://technet.microsoft.com/es-es/library/hh147307(v=ws.10).aspx*

Según lo señalado en ITILv3 indica que la Gestión de Accesos a los Servicios TI es el proceso por el cual a un usuario se le brindan los permisos necesarios para hacer uso de los servicios.[6]

Además de ello ITILv3 también señala que el **objetivo** de la Gestión de Acceso a los Servicios TI es otorgar permisos de acceso a los servicios a aquellos usuarios autorizados e impedírselo a los usuarios no autorizados.

2.2.1 VENTAJAS

ITILv3 también proporciona una serie de ventajas a la organización TI que justifican su implantación:

- Mayor garantía de confidencialidad de la información, gracias a un acceso controlado a los servicios.
- Mayor efectividad de los empleados, al minimizarse los conflictos y problemas derivados de la asignación de permisos.
- Menor probabilidad de errores en servicios críticos relacionados con la actividad de usuarios no cualificados.
- Capacidad de monitorizar el uso de los servicios y detectar casos de abuso de los mismos.
- Mayor rapidez y eficacia al revocar permisos en caso de ser necesario, algo que puede ser crítico para la seguridad en determinadas circunstancias.
- La Gestión de Acceso puede, además, ser un requisito indispensable para la adecuación a determinados estándares de calidad e incluso, a la legislación vigente (en el sector sanitario, por ejemplo).

Los principales retos a que se enfrenta habitualmente la Gestión de Acceso a los Servicios TI son:

- Verificar la identidad de los usuarios.
- Verificar la identidad de la persona u organismo que autoriza la asignación de permisos.
- Verificar que el usuario está solicitando el acceso a un determinado servicio.

---

[6] *http://itilv3.osiatis.es/operacion_servicios_TI/gestion_acceso_servicios_ti.php*

- Integrar múltiples niveles de permisos para un usuario concreto.
- Determinar con rapidez y fiabilidad el nivel de permisos del usuario en cualquier momento.
- Gestionar cambios en los requisitos de acceso de los usuarios.
- Restringir los permisos de acceso a los usuarios no autorizados.
- Mantener una base de datos actualizada donde figuren todos los usuarios y los derechos de los que gozan.

2.2.2 ROLES Y PERFILES DE USUARIOS

Como sabemos una organización está conformada por un conjunto de colaboradores que desempeña roles distintos según el cargo que tienen, es aquí que surge la necesidad de crear perfiles de usuarios teniendo en consideración las funciones y jerarquías que estos tienen, de acuerdo a ello se les otorgara una serie de accesos y privilegios a los recursos y servicios tecnológicos de la empresa.

ITILv3 considera en su glosario las siguientes definiciones para Rol y Perfil de Usuarios:

Rol de Usuario: Es un rol que forma parte de un catálogo o jerarquía de todos los roles (tipos de usuario) en la organización. Los derechos de acceso están basados en los roles que cada usuario individual tiene como parte de su organización.

Perfil de Usuario: Es un conjunto de datos que definen el nivel de acceso a un servicio o conjunto de servicios brindados a ciertos tipos de usuarios (Roles de Usuario). Los Perfiles de Acceso de Rol de Usuario sirven para proteger la confidencialidad, la integridad y la disponibilidad de los activos al definir qué información puede ser usada por los clientes, qué programas pueden usar y qué modificaciones pueden hacer.

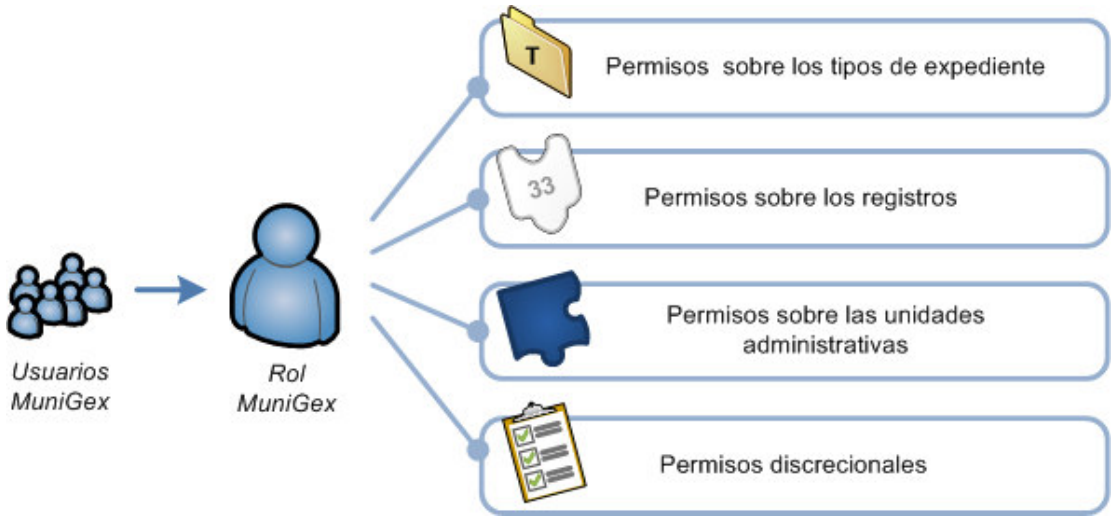


Ilustración 5: Roles y Permisos de Usuarios

Fuente: http://www.cgssl.es/MunigexHelp/manualBi/ES/Usuarios_permisos/Roles.htm

2.2.3 PROCESO DE GESTION DE ACCESOS:

Tomando como referencia el Marco de Servicios de TI de ITILV3 a continuación se describen los procesos que se deberían considerar como buenas prácticas en la Gestión de Accesos a los Servicios.
Las actividades de la Gestión de Acceso a los Servicios TI incluyen:

1. **Petición de acceso.** que puede llegar por distintas vías como el departamento de RRHH, una solicitud de cambio, una instrucción autorizada.

2. **Verificación.** Se comprueba la identidad del usuario que solicita el acceso, así como de aquellos que lo autorizan. También se examina si los motivos para otorgar el acceso son pertinentes.

3. **Monitorización de identidad.** Los cambios en la asignación de permisos suelen estar asociados a un cambio de estatus dentro de la organización: ascensos, despidos, jubilaciones.
4. **Registro y monitorización de accesos.** La Gestión de Accesos es responsable de asegurar que los permisos que ha otorgado se están usando apropiadamente.

5. **Eliminación y restricción de derechos.** En algunos casos, los derechos pueden ser eliminados por completo: fallecimiento, dimisión, despido, traslados.[7]

Ilustración 6: Procesos de la Gestión de Acceso-ITILv3

Fuente:
http://itilv3.osiatis.es/operacion_servicios_TI/gestion_acceso_servicios_ti/proceso.php

2.2.4 PROCESO DE GESTIÓN DE ACCESOS DE LA ENTIDAD BANCARIA EN ESTUDIO

La entidad bancaria actualmente posee un proceso de Gestión de Accesos que cuenta con unos conjuntos de procedimientos con flujos de atención de requerimientos, donde participan diversas áreas entre las cuales podemos destacar principalmente al Equipo de Soporte Usuario y la Subgerencia de Seguridad de la Información.

[7] *http://itilv3.osiatis.es/operacion_servicios_TI/gestion_acceso_servicios_ti/proceso.php*

2.2.4.1 Responsabilidades de la Gestión de Accesos

Según lo referenciado en el Manual de Control de Accesos MAN-RIE-101 se tienen las siguientes responsabilidades:

Equipo de Soporte Usuario

- Crear, modificar y eliminar las cuentas de los usuarios y perfiles de las aplicaciones core y no core.
- Implementar el esquema de perfiles consultando la Matriz de Recursos y Servicios de TI, brindada por la Subgerencia de Seguridad de la Información.

Subgerencia de Seguridad de la Información

- Establecer y administrar la matriz de Recursos y Servicios de TI y el detalle del perfil para cada aplicación.
- Realizar el monitoreo de las aplicaciones de acuerdo al cronograma de Monitoreos de Seguridad de la Información

2.2.4.2 Matrices de Gestión de Accesos

Para otorgar los accesos a los usuarios es necesario tener un registro de perfiles autorizados a las aplicaciones y recursos de TI, pues la guía principal de Soporte Usuario en la entrega de accesos, en la entidad bancaria se cuenta con 2 tipos de Matrices de Gestión de Perfiles:

- **Matriz Integral de Recursos y Servicios de TI:**
  Esta matriz es única y es la más importante pues detalla de manera general los cargos vs los perfiles de las aplicaciones que les corresponden a los usuarios, es el principal input para Soporte Usuario en la entrega de accesos.
- **Matriz de Detalla de Aplicaciones:**
  Esta matriz muestra el detalle de cada aplicativo donde se podrían establecer módulos, sub-módulos, opciones y sub-opciones, es un input para seguridad de la Información para realizar el monitoreo periódico de accesos a las aplicaciones.

2.2.4.3 Flujo Principal de la Gestión de Accesos

En la entidad Bancaria el flujo principal de la Gestión está asociado al **Procedimiento de la Creación de Usuarios en la Aplicaciones,** es en este flujo donde se encuentra la problemática del asunto pues aquí se otorgan los accesos a los colaboradores por primera vez.

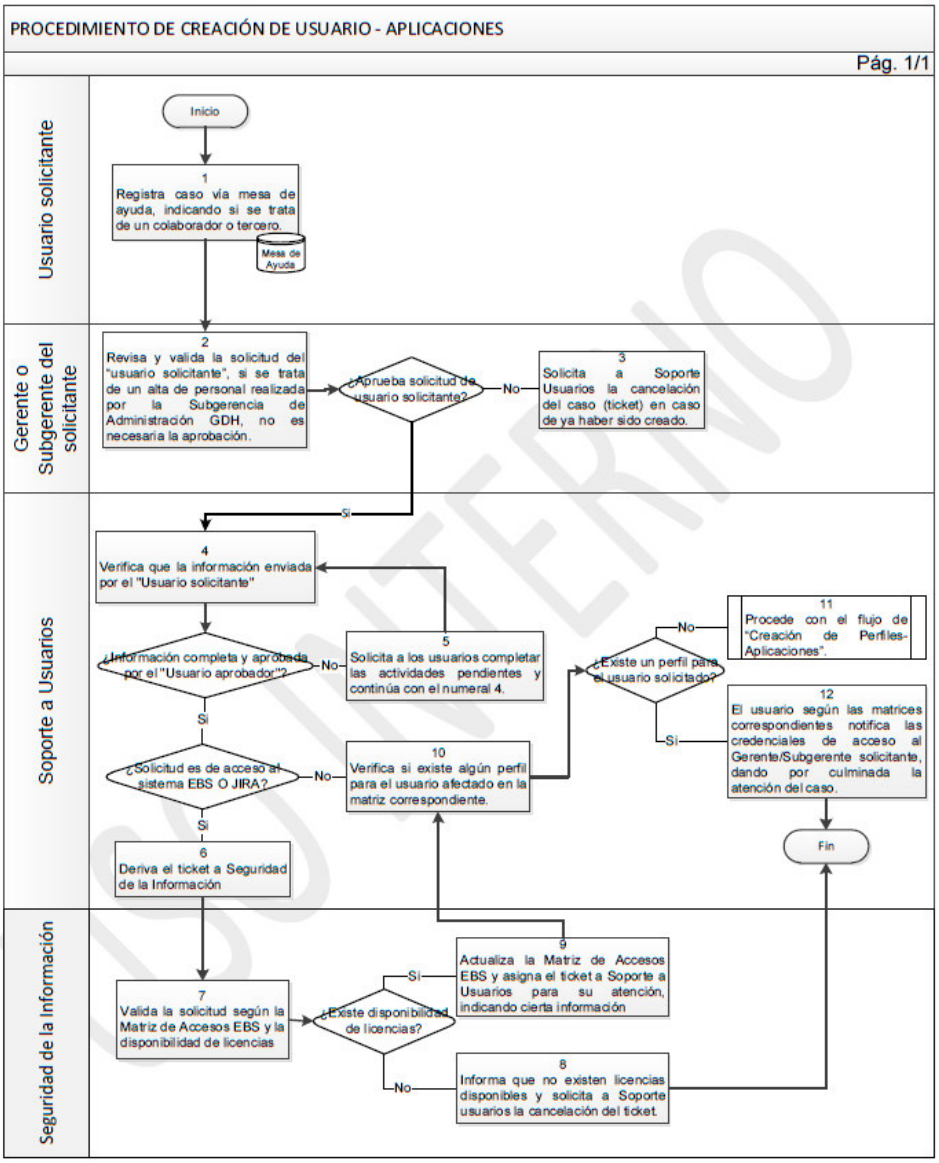


Ilustración 7: Flujo de Procedimiento de Creación de Usuarios

Fuente: Pág. 12 Manual de Control de Accesos MAN-RIE-101-Mibanco

2.3 SEGURIDAD DE LA INFORMACIÓN

2.3.1 DEFINICIÓN

Característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla los criterios de confidencialidad, integridad y disponibilidad. (Circular G-140-2009).

2.3.2 CRITERIOS DE SEGURIDAD DE LA INFORMACIÓN

- **Confidencialidad**: La información debe ser accesible sólo a aquellos que se encuentren debidamente autorizados.
- **Integridad**: La información debe ser completa, exacta y válida.
- **Disponibilidad**: La información debe estar disponible en forma organizada para los usuarios autorizados cuando sea requerida.

Ilustración 8: Principios básicos de la Seguridad de la Información

Fuente: http://institucion.ean.edu.co/seccion/seguridad-de-la-informacion.html

2.3.3 NORMAS Y ESTANDARES DE SEGURIDAD DE LA INFORMACIÓN

2.3.3.1 Estándar Internacional ISO/IEC 27001

Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI.

Actualmente, la última edición de 2013 este estándar se encuentra en inglés y en francés tras su acuerdo de publicación el 25 de Septiembre de 2013. Desde el 12 de Noviembre de 2014, esta norma está publicada en España como UNE-ISO/IEC 27001:2014 y puede adquirirse online en AENOR. En 2015, se publicó un documento adicional de modificaciones (UNE-ISO/IEC 27001:2014/Cor 1:2015). Otros países donde también está publicada en español son, por ejemplo, Colombia (NTC-ISO-IEC 27001), Chile (NCh-ISO27001) o Uruguay (UNIT-ISO/IEC 27001).[8]

Ilustración 9: Dominios de la ISO/IEC 27001

Fuente:https://oscargiudice.wordpress.com/2012/03/25/la-norma-isoiec-27002-seguridad-de-la-inf

[8] *http://www.iso27000.es/iso27000.html*

2.3.3.2 CIRCULAR Nº G- 140 -2009:

Es la norma emitida por la Superintendencia de Banca y Seguros del Perú SBS, publicada el 06 de abril de 2009 en el diario el peruano que señala que todas las entidades que estén bajo su regulación deberán establecer, mantener y documentar un sistema de gestión de la seguridad de la información (SGSI), toma como referencia

Estándares internacionales como el ISO 17799 e ISO 27001.

A continuación se muestran 2 de los artículos más importantes:

Artículo 1º.- *La presente Circular será de aplicación a las empresas señaladas en los artículos 16° y 17° de la Ley General, así como a las Administradoras Privadas de Fondos de Pensiones (AFP), en adelante empresas. También será de aplicación a las Cajas Municipales de Ahorro y Crédito (CMAC), la Caja Municipal de Crédito Popular, el Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI), el Banco de la Nación, el Banco Agropecuario, la Corporación Financiera de Desarrollo (COFIDE), el Fondo MIVIVIENDA S.A., y las Derramas y Cajas de Beneficios bajo control de la Superintendencia, la Federación Peruana de Cajas Municipales de Ahorro y Crédito (FEPCMAC) y el Fondo de Cajas Municipales de Ahorro y Crédito (FOCMAC), en tanto no se contrapongan con las normativas específicas que regulen el accionar de estas empresas.*[9]

Artículo 3º.- *Las empresas deberán establecer, mantener y documentar un sistema de gestión de la seguridad de la información (SGSI).*

Las actividades mínimas que deben desarrollarse para implementar el SGSI, son las siguientes:

a. Definición de una política de seguridad de información aprobada por el Directorio.

b. Definición e implementación de una metodología de gestión de riesgos, que guarde consistencia con la gestión de riesgos operacionales de la empresa.

[9] *Artículo 1; Pág. 1; Circular G-140-2009-SBS*

c. Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la empresa, así como mantener pistas adecuadas de auditoría.[10]

2.3.3.3 Norma Técnica Peruana "NTP-ISO/ IEC 17799:2007

NTP-ISO/ IEC 17799:2007-Código de buenas prácticas para la gestión de la seguridad de la información en todas las Entidades integrantes del Sistema Nacional de Informática, publicada en el Diario el Peruano el 22 de agosto de 2007, toma como referencia el estándar internacional como el ISO 17799.

[10] *Articulo 3; Pág. 2; Circular G-140-2009-SBS*

Capítulo 3: ESTADO DEL ARTE

3.1 TAXONOMIA

No se encontró referencias de la clasificación del problema, por el cual se plantea una taxonomía de acuerdo a juicio de experto.

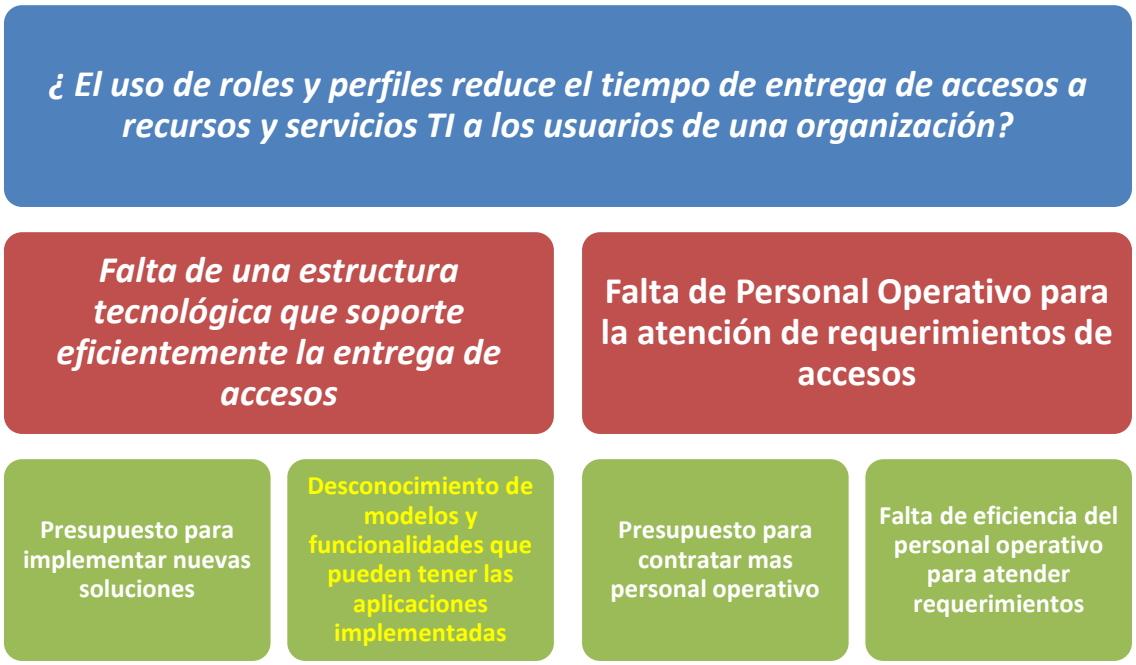


Ilustración 10: Taxonomía del Problema

Fuente: Creación Propia

En la figura anterior se ha querido encontrar la causa principal del problema mediante el uso de una taxonomía de clasificación de problemas y se llega a la conclusión que esta se da por el *"Desconocimiento de modelos y funcionalidades que pueden tener los aplicativos ya implementados*", cabe señalar que esta creación es propia por lo cual es solo referencial para fines del trabajo.

3.2 METODOS-MODELOS

No se han encontrado referencias de modelos o metodologías para la creación de estructuras de grupos o perfiles en Servicios de directorios, por lo cual se describirá el método propio para la implementación de la Solución.

Ilustración 11: Metodología de Implementación de Grupos en SD

Fuente: Creación Propia

1. **Identificación del Patrón Jerárquico de la Estructura Organizativa**

   En esta etapa se busca identificar el patrón de jerarquías de la Organización, es decir cómo está divida la empresa, esto servirá para conocer todos los niveles existe que se tienen que diseñar.

2. **Creación de Estructura organizativa de grupos según Patrón Jerárquico**

   En esta etapa se crea en AD la estructura organizativa de grupos de acuerdo al patrón jerárquico, se debe tener en cuenta que el grupo de menor nivel es un grupo asociado al cargo de un usuario.

3. **Creación de grupos de accesos a Recursos y Servicios según Políticas**

   En esta etapa se debe de crear todos los grupos que pueden integrarse en el AD, se debe tener de input las políticas de accesos a los recursos y servicios.

4. **Integración de grupos organizativos con grupos de accesos a Recursos y Servicios TI**

   En esta etapa se integran los grupos organizativos con los grupos de acceso a recursos, esos quiere decir que el grupo organizativo ya tiene integrado accesos a servicios por la herencia de grupos AD.

5. **Implementación de Estructura Lógica de Grupos en Servicio de Directorio**

   Esta es la etapa final donde se realiza la implementación de la Estructura Lógica de grupos de accesos (matrices de roles y perfiles) en la aplicación de Servicio de Directorio seleccionado.

3.3 APLICATIVOS

Existen muchas soluciones de Servicios de Directorios en aplicaciones ya sean licenciadas o software libre que corre en código abierto, para fines de la solución del problema es necesario elegir aquellos que tengan una buena gestión de usuarios, gestión de grupos y gestión de directivas de Seguridad, pues el fin es restringir accesos a los recursos y servicios de TI, en el marco teórico ya se explicó sobre Active Directory a ahora se realizará el estudio de aplicaciones de código que tienen funcionalidades similares.

3.3.1 LDAP (PROTOCOLO LIGERO DE ACCESO A DIRECTORIOS)

Es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red, este protocolo también es considerado como una base de datos.

Como funciona un LDAP

Este se basa de un modelo cliente-servidor. Uno o más servidores LDAP contienen los datos que conforman el árbol del directorio LDAP o base de datos troncal, el cliente LDAP se conecta con el servidor LDAP y le hace una consulta, el servidor

contesta con la respuesta correspondiente o con una identificación que el cliente puede hallar más información (otro servidor LDAP)

Ilustración 12: Funcionamiento del protocolo LADP

Fuente: https://www.qnap.com/static/es/fw_v35/ldap.html

3.3.2 SAMBA

Samba es una suite de aplicaciones de software libre que utiliza el protocolo SMB (Server Message Block) compatible con Windows NT 4. Samba permite a las máquinas Unix comunicarse con el mismo protocolo de red que Microsoft Windows y aparecer como otro sistema Windows en la red (desde la perspectiva de un cliente Windows). [11] El servidor Samba ofrece los siguientes servicios:

- Compartir uno o varios sistemas de archivos
- Compartir uno o varios sistemas de archivos distribuidos
- Compartir impresoras instaladas en el servidor entre los clientes Windows de la red
- Ayudar a los clientes permitiéndoles navegar por la red
- Autentificar a los clientes que ingresan en un dominio Windows
- Proveer o ayudar con un servidor de resolución de nombres Windows (WINS)

[11] "Implementación de un Servidor Samba con autenticación LDAP como alternativa Libre a los Servidores de Dominio Windows"; Ing. Lázaro Ramos - MSc. Miriel Martín; Pág. 16.

La suite Samba gira alrededor de un par de demonios Unix que permiten la compartición de recursos entre los clientes SMB de una red. Estos demonios son:

Smbd: Permite la compartición de archivos e impresoras sobre una red SMB y proporciona autentificación y autorización de acceso para clientes SMB.

Nmbd: Soporta el servicio de nombres NetBIOS y WINS, que es una implementación de Microsoft del servicio de nombres NetBIOS (NBNS). Este demonio también ayuda añadiendo la posibilidad de navegar por la red.

3.3.3 KERBEROS

Es un protocolo de autenticación que tiene una arquitectura cliente-servidor que proporciona seguridad a las transacciones en las redes. La autenticación garantiza que las identidades del remitente y del destinatario de las transacciones de la red sean verdaderas. El servicio también puede verificar la validez de los datos que se transfieren de un lugar a otro (integridad) y cifrar los datos durante la transmisión (privacidad). El servicio Kerberos funciona en base al concepto de tickets que es un conjunto de información electrónica que identifica a un usuario o servicio. Con el servicio Kerberos se puede iniciar sesión en otros equipos, ejecutar comandos, intercambiar datos y transferir archivos de manera segura. [12]

Servicio de Seguridad de KERBEROS

El servicio Kerberos proporciona dos servicios de seguridad:

Integridad: Garantiza que los datos que estos envían sean válidos y que no se hayan alterado durante la transmisión.

Privacidad: Cifra los datos antes de la transmisión para protegerlos de los usuarios no autorizados.

[12] https://docs.oracle.com/cd/E24842_01/html/E23286/intro-5.html#scrolltoc

3.3.4 COMPARATIVA ENTRE LDAP, SAMBA, KERBEROS Y ACTIVE DIRECTORY

	Funcionalidades\Servicios de Directorio	LDAP (SW Libre)	SAMBA (SW Libre)	KERBEROS (SW Libre)	Active Directory (SW Licenciado)
1	*Gestión de Objetos y Grupos (Usuarios, Equipos y OU)*	Si	Si	Si	Si
2	*Gestión de Directivas de Seguridad (Políticas)*	Si	Si	Si	Si
3	*Integración de Servicios de TI*	Si	Si	Si	Si
4	*Compatibilidad con Windows*	Si	Si	Si	Si
5	*Multiplataformas*	Si	Si	Si	No
6	*Proveedores de mantenimiento*	No	No	No	Si
7	*Instalación Anterior en el Banco*	No	No	No	Si

Ilustración 13: Comparativas entre LDAP, SAMBA, KERBEROS y AD

Fuente: Creación Propia

Se ha realizado un análisis de las funcionalidades importantes para la implementación de un Servicio de Directorio para aplicativos de codigo abierto como LDAP, Samba y Kerberos y licenciados como Active Directory, si bien es cierto cada uno presenta características similares, lo ideal es elegir el que más se acomode a las necesidades de la empresa, en el caso nuestro se mantendrá la estructura de Active Directory por los siguientes razones:

- Compatibilidad de la mayoría de los servicios y recursos TI (correos, nivel de internet, dispositivos usb y directorios Compartidos) ya están implementados con tecnología Windows.
- Las directivas de Seguridad de Active Directory son más configurables para restringir accesos.
- El mantenimiento que puede tener un Servicio de Directorio de un aplicativo licenciado como Windows Server.
- Familiarización con el aplicativo pues anteriormente ya se instaló y su funcionamiento es conocido en detalla por el equipo de Administración de Redes y Comunicaciones.

Capítulo 4: PROPUESTA : MODELO TEÓRICO

4.1 MÉTODO DE INTEGRACIÓN USANDO GRUPOS DE SEGURIDAD EN SERVICIOS DE DIRECTORIOS

Ilustración 14: Etapas del método de Implementación de Grupos en SD

Fuente: Creación Propia

ETAPAS

1. **Etapa 1: Identificación del Patrón Jerárquico de la Estructura Organizativa**

   En esta etapa se busca identificar el patrón de jerarquías de la Organización, es decir cómo está divida la empresa, esto servirá para conocer todos los niveles existe que se tienen que diseñar.

2. **Etapa 2: Creación de Estructura organizativa de grupos según Patrón Jerárquico**

   En esta etapa se crea en AD la estructura organizativa de grupos de acuerdo al patrón jerárquico, se debe tener en cuenta que el grupo de menor nivel es un grupo asociado al cargo de un usuario.

3. **Etapa 3: Creación de grupos de accesos a Recursos y Servicios según Políticas**

   En esta etapa se debe de crear todos los grupos que pueden integrarse en el AD, se debe tener de input las políticas de accesos a los recursos y servicios.

4. **Etapa 4: Integración de grupos organizativos con grupos de accesos a Recursos y Servicios TI**

   En esta etapa se integran los grupos organizativos con los grupos de acceso a recursos, esos quiere decir que el grupo organizativo ya tiene integrado accesos a servicios por la herencia de grupos AD.

5. **Etapa 5: Implementación de Estructura Lógica de Grupos en Servicio de Directorio**

   Esta es la etapa final donde se realiza la implementación de la Estructura Lógica de grupos de accesos (matrices de roles y perfiles) en la aplicación de Servicio de Directorio seleccionado.

4.2 PLAN DE TRABAJO PARA LA IMPLEMENTACIÓN

4.2.1 Estructura de Desglose del Trabajo-EDT

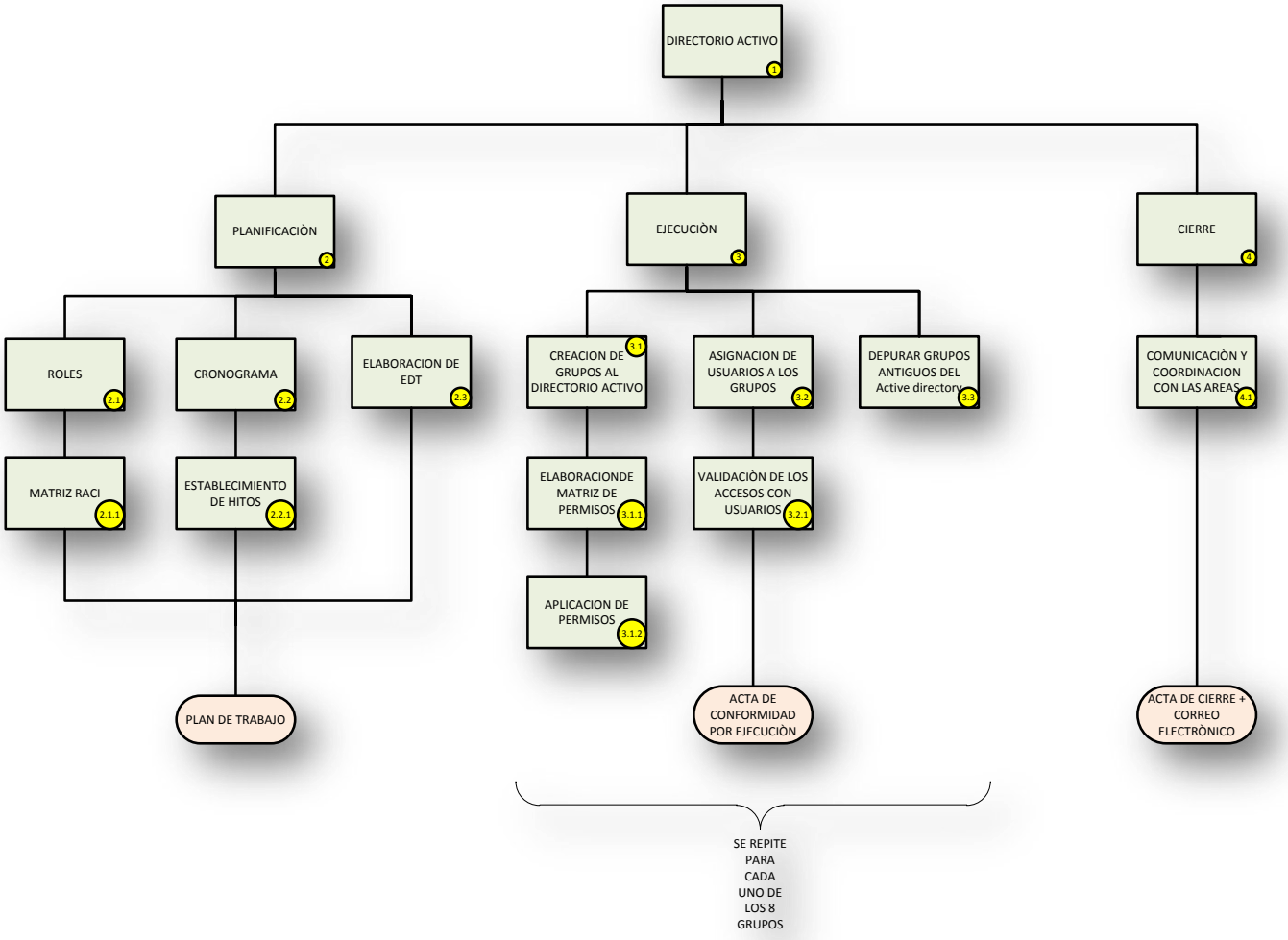


Ilustración 15: Estructura EDT

Fuente: Basada en el Acta de Constitución de Proyecto Mibanco 2015

4.2.2 Recursos Humanos

4.2.2.1 Estructura del Proyecto

A continuación se muestra la estructura del proyecto:

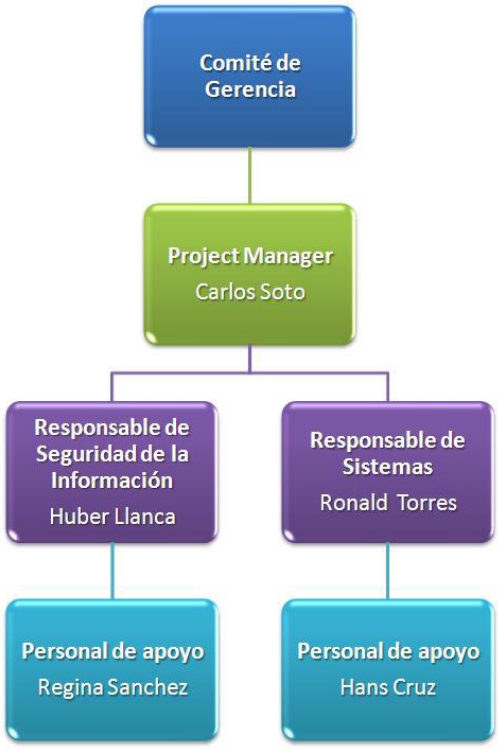


Ilustración 16: Equipo de Proyecto

Fuente: Basada en el Acta de Constitución de Proyecto Mibanco 2015

4.2.2.2 Roles

A continuación se listan los principales roles:

Ítem	Rol / Función	Área / Proveedor	Responsable	Condición
1.	**Project Manager**	**Seguridad de la Información**	**Jefe de Seguridad de la Información**	**Contratado**
2.	Responsable de Sistemas	Sistemas	Administrador de Redes	Contratado

			y Comunicaciones 1	
3.	Personal de Apoyo – Sistemas	Sistemas	Administrador de Redes y Comunicaciones 2	Contratado
4.	Responsable de Seguridad de la Información	Seguridad de la Información	Analista de Seguridad de la Información 1	Contratado
5.	Personal de Apoyo – SI	Seguridad de la Información	Analista de Seguridad de la Información 2	Contratado

Ilustración 17 : Cuadro de Roles del Proyecto

Fuente: Basada en el Acta de Constitución de Proyecto Mibanco 2015

4.2.2.3 Responsabilidades

A continuación se listan las principales responsabilidades:

Ítem	Tarea	Responsable
1.	Creación de los grupos en el Active Directory	Administrador de Redes y Comunicaciones 1
2.	Asignación de los usuarios a los grupos	Analista de Seguridad de la Información 1
4.	Elaboración matriz de permisos – Etapas 1-5	Analista de Seguridad de la Información 1
5.	Aplicación de permisos – Etapas 1-5	Administrador de Redes y Comunicaciones 1
6.	Validación de Permisos con los Usuarios	Analista de Seguridad de la Información 1
7.	Elaboración de Actas de conformidad	Jefe de Seguridad de la Información
8.	Depuración de grupos del Active Directory	Administrador de Redes y Comunicaciones 2
9.	Elaboración de acta de Cierre	Jefe de Seguridad de la Información

Ilustración 18 : Cuadro de Responsabilidades del Proyecto

Fuente: Basada en el Acta de Constitución de Proyecto Mibanco 2015

WBS	Actividad	Responsable	Duración	Inicio	Fin
1	**Planificación**		**9 días**	**27/01/2015**	**05/02/2015**
1.1	Análisis y definición de actividades a realizar	Analista de SI 1	3 días	27/01/2015	29/01/2015
1.2	Elaboración del plan de trabajo	Analista de SI 1	5 días	28/01/2015	05/02/2015
1.3	Entregable: Plan de Trabajo	Analista de SI 1	1 días	05/02/2015	05/02/2015
2	**Active Directory**		**23 días**	**23/02/2015**	**23/03/2015**
2.1	Definición de Estructura Propuesta	Analista de SI 1	10 días	23/02/2015	04/03/2015
2.2	Validación de Estructura de Grupos con RC e IP	Analista de SI 1	5 días	07/03/2015	11/03/2015
2.3	Creación de los grupos en el Directorio Activo	Administrador de RyC 1	4 días	14/03/2015	17/03/2015
2.4	Asignación de los Usuarios a los grupos	Administrador de RyC 1 Analista de SI 1	3 días	18/03/2015	22/03/2015
2.5	Acta de Conformidad	Analista de SI 1	1 días	23/03/2015	23/03/2015
3	**Share point**		**33 días**	**24/03/2015**	**27/04/2015**
3.1	Elaboración de Matriz de Permisos	Analista de SI 1	6 días	24/03/2015	31/03/2015
3.2	Validación de accesos con Usuarios.	Analista de SI 1	17 días	13/03/2015	05/04/2015
3.3	Aplicación de permisos.	Administrador de RyC 1	6 días	06/04/2015	13/04/2015
3.4	Entregable: Acta de Conformidad por Gerencias	Analista de SI 1	4 días	24/04/2015	27/04/2015
4	**WLAN/DLP Puertos**		**28 días**	**01/04/2015**	**27/05/2015**
4.1	Elaboración de Matriz de Permisos	Analista de SI 1	4 días	01/04/2015	06/04/2015
4.2	Validación de accesos con Usuarios.	Analista de SI 1	17 días	13/04/2015	05/05/2015
4.3	Aplicación de permisos.	Administrador de RyC 1	3 días	16/05/2015	18/05/2015
4.4	Entregable: Acta de Conformidad por Gerencias	Analista de SI 1	4 días	24/05/2015	27/05/2015
5	**Correo Electrónico/Internet**		**28 días**	**07/04/2015**	**27/05/2015**
5.1	Elaboración de Matriz de Permisos	Analista de SI 1	4 días	07/04/2015	12/04/2015
5.2	Validación de accesos con Usuarios.	Analista de SI 1	17 días	13/05/2015	05/05/2015
5.3	Aplicación de permisos.	Administrador de RyC 1	3 días	19/05/2015	23/05/2015
5.4	Entregable: Acta de Conformidad por Gerencias	Analista de SI 1	4 días	24/05/2015	27/05/2015
6	**Cierre de Proyecto**		**2 días**	**30/05/2015**	**31/05/2015**
6.1	Entregable: Acta de Cierre.	Analista de SI 1	2 días	30/05/2015	31/05/2015

Ilustración 19: Cronograma del Proyecto

Fuente: Basada en el Acta de Constitución de Proyecto Mibanco 2015

4.3 CONSTRUCCIÓN LÓGICA APLICANDO INGENIERÍA DE ROLES Y PERFILES.

4.3.1 Estructura Organizativa de la Entidad Bancaria-Etapa 1

En esta etapa de la resolución se va identificar el patrón jerárquico de la organización y se va mapear todo en un estructura organizativa.

Para obtener este patrón tenemos como entrada el organigrama de la empresa que se muestra en el **Anexo 1: Estructura Organizativa del Banco.**

La Entidad Bancaria está representada jerárquicamente por el siguiente Árbol:

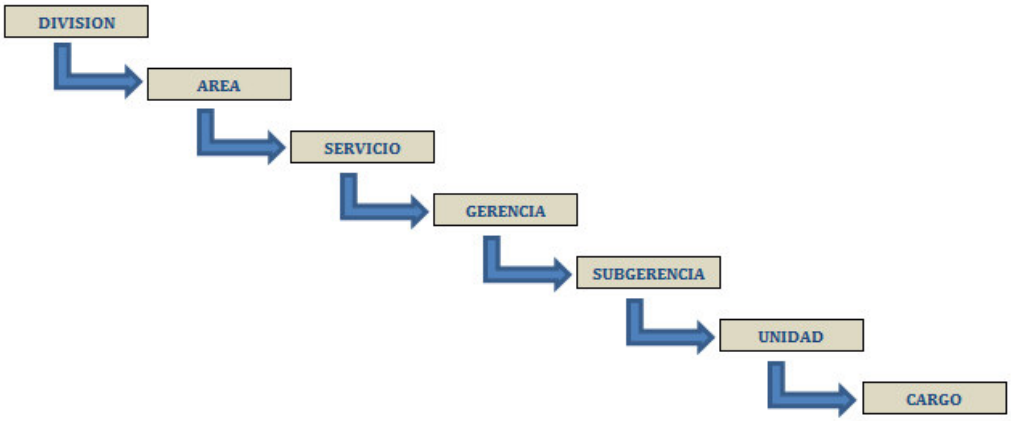


Ilustración 20: Patrón Jerárquico de la Organización

Fuente: Creación Propia

Aquí se tiene un ejemplo de una estructura jerárquica de cargos de un Servicio:

SERVICIO DE RO Y GESTION DE FRAUDES

GERENTE DE SERVICIO DE RO Y GESTION DE FRAUDES

UNIDAD DE CONTINUIDAD DE NEGOCIO
SUBGERENTE DE CONTINUIDAD DEL NEGOCIO
ANALISTA SENIOR DE CONTINUIDAD DEL NEGOCIOS
ANALISTA DE CONTINUIDAD DEL NEGOCIO

UNIDAD DE PREVENCION DE FRAUDES
SUBGERENTE DE PREVENCION DE FRAUDES
ANALISTA DE PREVENCION DE FRAUDES

UNIDAD DE RIESGO OPERATIVO
SUBGERENTE DE RIESGO OPERATIVO
ANALISTA SENIOR DE RIESGO OPERATIVO
ANALISTA DE RIESGO OPERATIVO

UNIDAD DE SEGURIDAD DE LA INFORMACION
SUBGERENTE DE SEGURIDAD DE LA INFORMACION
ANALISTA SENIOR DE SEGURIDAD DE LA INFORMACION
ANALISTA DE SEGURIDAD DE LA INFORMACION
PRACTICANTE DE SEGURIDAD DE LA INFORMACION

Ilustración 21: Estructura Jerárquica del Servicio de RO y Gestión de Fraudes

Fuente: Basada en la Matriz Integral AD-Mibanco

4.3.2 Creación de Grupos de Seguridad de Puestos estableciendo nivel de Jerarquías -Etapa 2

En esta etapa de la resolución se va a crear la estructura de Grupos de Seguridad asociados a al patrón organizativo de la empresa.

Tipos de Grupos

Grupos Unidad:

También llamados grupos contenedores o padres y según el organigrama serán representados por las siguientes jerarquías: División, Área, Servicio, Gerencia, Subgerencia y Unidad

***Nomenclatura*: G_Acrónimo-Unidad**

Acrónimo-Unidad: Representa la abreviatura de descripción de una División, Área, Servicio, Gerencia, Subgerencia o Unidad.

Ejemplo:

Descripción de Nombre	Nombre Grupo
DIVISION DE ADMINISTRACION	**G_DIV_ADM**

Acrónimo-Unidad: DIV_ADM

Grupos Cargos:

También llamados grupos hojas pues son el último nivel de grupos creados, está representado por los grupos de cargos que contienen a los usuarios.

Nomenclatura : G_Código-Puesto

Código-Puesto:

Representa el código único que posee un puesto, este se genera en el aplicativo de Recursos Humanos.

Ejemplo:

Descripción de Nombre	Nombre Grupo
GERENTE DE DIVISION DE ADMINISTRACION	**G_0000758**

Código-Puesto: **0000758**

Aquí se tiene un ejemplo de una estructura jerárquica de grupo de un Servicio donde se puede observar los tipos de grupos y las nomenclaturas, para mayor detalle se tiene el **Anexo 2: Estructura de Grupos de Seguridad del Banco.**

ESTRUCTURA JERARQUICA	COD GRUPO	TIPO DE GRUPO
SERVICIO DE RO Y GESTION DE FRAUDES	G_RIE_ROF	GRUPO UNIDAD
GERENTE DE SERVICIO DE RO Y GESTION DE FRAUDES	G_00000788	GRUPO CARGO
UNIDAD DE CONTINUIDAD DE NEGOCIO	G_ROF_CDN	GRUPO UNIDAD
SUBGERENTE DE CONTINUIDAD DEL NEGOCIO	G_00000618	GRUPO CARGO
ANALISTA SENIOR DE CONTINUIDAD DEL NEGOCIOS	G_00000318	GRUPO CARGO
ANALISTA DE CONTINUIDAD DEL NEGOCIO	G_00000807	GRUPO CARGO
UNIDAD DE PREVENCION DE FRAUDES	G_ROF_FRA	GRUPO UNIDAD
SUBGERENTE DE PREVENCION DE FRAUDES	G_00000590	GRUPO CARGO
ANALISTA DE PREVENCION DE FRAUDES	G_00000827	GRUPO CARGO
UNIDAD DE RIESGO OPERATIVO	G_ROF_ROP	GRUPO UNIDAD
SUBGERENTE DE RIESGO OPERATIVO	G_00000596	GRUPO CARGO
ANALISTA SENIOR DE RIESGO OPERATIVO	G_00000650	GRUPO CARGO
ANALISTA DE RIESGO OPERATIVO	G_00000831	GRUPO CARGO
UNIDAD DE SEGURIDAD DE LA INFORMACION	G_ROF_SIN	GRUPO UNIDAD
SUBGERENTE DE SEGURIDAD DE LA INFORMACION	G_00000149	GRUPO CARGO
ANALISTA SENIOR DE SEGURIDAD DE LA INFORMACION	G_00000651	GRUPO CARGO
ANALISTA DE SEGURIDAD DE LA INFORMACION	G_00000832	GRUPO CARGO
PRACTICANTE DE SEGURIDAD DE LA INFORMACION	G_00000866	GRUPO CARGO

Ilustración 22: Estructura de Grupos de Seguridad de Servicio de RO y Gestión de Fraudes

Fuente: Basada en la Matriz Integral AD-Mibanco

4.3.3 Integrar los Servicios de TI a los grupos de Active Directory-Etapa 3 y 4

En esta etapa de la resolución se identificó los siguientes servicios y recursos de TI que se pueden integrar a AD que son los siguientes: *Internet, Correo Electrónico, Dispositivos USB y Directorios Compartidos.* Además de ello se crearon los grupos de seguridad de todos los atributos que puedan tener estos servicios y recursos TI.

Ejemplo: En la ilustración 23 se puede observar grupos de servicios como el de internet que cuenta con diversos grupos de acuerdo a niveles establecidos según las políticas de navegación: IUser Nivel 0,1, y 2.

ANEXO 3: Estructura Integral de Grupos AD vs Servicios de TI

		INTERNET		ATRIBUTOS DE CORREO				DISP. USB	DIRECTORIOS COMPARTIDOS								
Nombre Grup	Descripción de Nombre	NIVELES	WIRELESS	SALIDA EXTERNA	ALMACENAMIENTO	ENVIO INTERNO	ENVIÓ EXTERNO	NIVELES	PRIV_MIBANCO	PRIV_OFICINA PRINCIPAL	PRIV_DIV. ADMINISTRACION	PRIV_DIV. AUDITORIA INTERNA	PRIV_DIV. FINANZAS	PRIV_DIV. GDH	PRIV_DIV. GERENCIA GENERAL	PRIV_DIV. GERENCIA GENERAL	PRIV_DIV. LEGAL
G_RIE_ROF	SERVICIO DE RO Y GESTION DE FRAUDES																
G_00000788	GERENTE DE SERVICIO DE RO Y GESTION DE FRAUDES	IUser Nivel 0	Sí	Sí	GRUPO A	10 MB	3 MB	USB_BloqueoTotal									
G_ROF_CDN	UNIDAD DE CONTINUIDAD DE NEGOCIO																
G_00000618	ANALISTA SENIOR DE CONTINUIDAD DEL NEGOCIO	IUser Nivel 1	Sí	Sí	GRUPO D	5 MB	3 MB	USB_BloqueoTotal									
G_00000318	ANALISTA DE CONTINUIDAD DEL NEGOCIO	IUser Nivel 2	Sí					USB_BloqueoTotal									
G_00000807	SUBGERENTE DE CONTINUIDAD DEL NEGOCIO	IUser Nivel 1	Sí	Sí	GRUPO C	5 MB	3 MB	USB_BloqueoTotal									
G_ROF_FRA	UNIDAD DE PREVENCION DE FRAUDES																
G_00000590	ANALISTA DE PREVENCION DE FRAUDES	IUser Nivel 2	Sí	No	GRUPO D	5 MB	Restringido	USB_BloqueoTotal									
G_00000827	SUBGERENTE DE PREVENCION DE FRAUDES	IUser Nivel 1	Sí	Sí	GRUPO C	5 MB	Restringido	USB_BloqueoTotal									
G_ROF_ROP	UNIDAD DE RIESGO OPERATIVO																
G_00000596	ANALISTA DE RIESGO OPERATIVO	IUser Nivel 2	Sí	Sí	GRUPO D	5 MB	3 MB	USB_BloqueoTotal									
G_00000650	ANALISTA SENIOR DE RIESGO OPERATIVO	IUser Nivel 1	Sí	Sí	GRUPO D	5 MB	3 MB	USB_BloqueoTotal									
G_00000831	SUBGERENTE DE RIESGO OPERATIVO	IUser Nivel 1	Sí	Sí	GRUPO C	5 MB	3 MB	USB_BloqueoTotal									
G_ROF_SIN	UNIDAD DE SEGURIDAD DE LA INFORMACION																
G_00000149	ANALISTA DE SEGURIDAD DE LA INFORMACION	IUser Nivel 2	Sí	Sí	GRUPO D	5 MB	3 MB	USB_SoloLectura									
G_00000651	ANALISTA SENIOR DE SEGURIDAD DE LA INFORMACION	IUser Nivel 1	Sí	Sí	GRUPO D	5 MB	3 MB	USB_SoloLectura									
G_00000832	SUBGERENTE DE SEGURIDAD DE LA INFORMACION	IUser Nivel 1	Sí	Sí	GRUPO C	5 MB	3 MB	USB_SoloLectura									
G_00000866	PRACTICANTE DE SEGURIDAD DE LA INFORMACION	IUser Nivel 2	No	No	GRUPO D	5 MB	Restringido	USB_BloqueoTotal									

Ilustración 23: Estructura Integral de Grupos AD vs Servicios de TI del Servicio de RO y Gestión de Fraudes

Fuente: Basada en la Matriz Integral AD-Mibanco

Capítulo 5: CASO DE ESTUDIO (VALIDACIÓN Y PRUEBAS)

5.1 DESCRIPCIÓN DEL AMBIENTE DEL CASO DE ESTUDIO

Previo a la etapa de implementación es necesario realizar un conjunto de pruebas para asegurarnos el buen funcionamiento de los grupos de seguridad configurados, para ello se utilizará un servidor de pruebas donde utilizará el software de virtualización Vmware en él se instalará Windows Server 2012 Standar la misma versión que posee la organización en estudio, se realizarán las configuraciones necesaria para tener el Active Directory operativo.

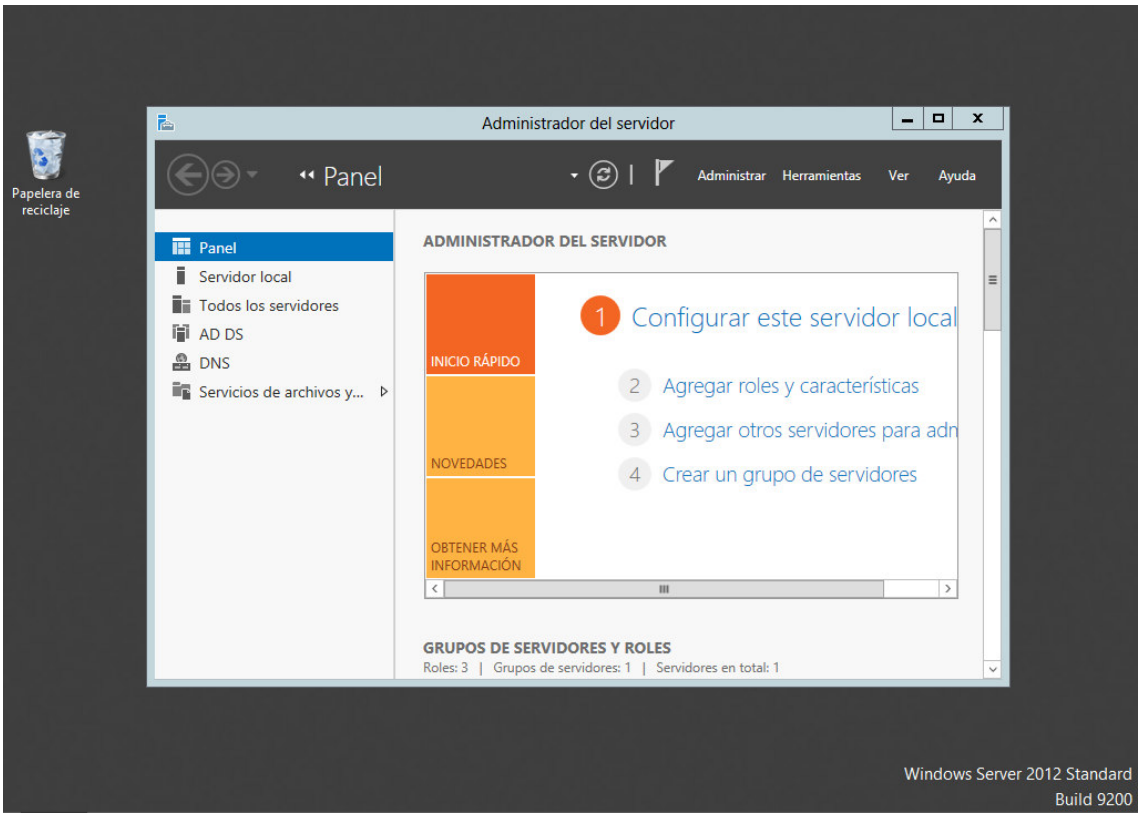


Ilustración 24: Configuración de Active Directory en Windows Server 2012

Fuente: Creación Propia

5.2 DISEÑO DE LAS PRUEBAS, EXPERIMENTOS Y/O VALIDACIÓN

5.2.1 Diseño de Pruebas

Como no se trata de un desarrollo de software el diseño de pruebas no es tan complejo pero si operativo, la elaboración de la mismas está más orientado al correcto funcionamiento de la políticas de accesos configuradas en Active Directory, para ello se usaran **pruebas de validación alfa**.

"La prueba alfa se lleva a cabo en el sitio del desarrollador por un grupo representativo de usuarios finales. El software se usa en un escenario natural con el desarrollador "mirando sobre el hombro" de los usuarios y registrando los errores y problemas de uso. Las pruebas alfa se realizan en un ambiente controlado".[13]

5.2.2 Caso de Pruebas

Los casos de pruebas que se van a desarrollar tienen el objetivo de encontrar observaciones en la configuración de accesos de los usuarios según el perfil asociado al grupo de seguridad AD y lo servicios integrados a él.

Caso de Prueba n	**Revisar si un usuario Ux con cargo Cx tiene acceso al servicio Sx según la matriz integral de grupos AD**
Objetivo	Comprobar que el acceso configurado al servicio le corresponde según el cargo que posee.
Requisitos previos	El usuario debe haber iniciado sesión con su cuenta Windows en la estación de trabajo.
Datos de entrada	Los datos estas asociado de acuerdo al tipo de servicio Sx que se va probar.

[13] Pressman, R. (2010). Estrategias de prueba de software. En Ingeniería del software: un enfoque práctico (pp. 4)

Pasos a seguir	Los pasos están asociados de acuerdo al tipo de servicio Sx que se va probar.
Resultado esperado	Los resultados están asociados de acuerdo al tipo de servicio Sx que se va probar.

Ilustración 25: Modelo de plantilla caso de prueba.

Fuente: Creación adecuada buenas prácticas de prueba de software

5.3 RESULTADOS

Como sabemos el alcance de servicios que se van a configurar son: *Internet, Correo Electrónico, Dispositivos USB y Directorios Compartidos,* en esta oportunidad tomaremos como ejemplo el servicio de correo Outlook.

5.3.1 Caso de Prueba de Servicios de Correo

Caso de Prueba 1	**Revisar si un usuario con cargo Cx tiene acceso al servicio de correo con los atributos de envió y recepción interno y externo según la matriz integral de grupos AD**
Objetivo	Comprobar que el acceso configurado al servicio de correo para los atributos de envió y recepción corresponde al cargo que posee según la matriz de grupos de active directory.
Requisitos previos	El usuario debe haber iniciado sesión con su cuenta Windows en la estación de trabajo.
Datos de entrada	Revisar la matriz de grupos de active directory, identificar el grupo del Cargo Cx, y revisar los atributos de envío y recepción que posee.
Pasos a seguir	1.1. Enviar correos internos y externos con una capacidad menor o igual al establecido. 1.2. Enviar correos internos y externos con una capacidad mayor al establecido. 2.1. Recepcionar correos internos y externos con una capacidad

	menor o igual al establecido. 2.2. Recepcionar internos y externos con una capacidad mayor al establecido.
Resultado esperado	1.1. Envío de correo exitoso a cuenta de correo interna. 1.2. Envío de correo fallido a cuenta de correo interna. 1.3. Envío de correo exitoso a cuenta de correo externa. 1.4. Envío de correo fallido a cuenta de correo externa. 2.1. Recepción de correo exitoso por cuenta de correo interna. 2.2. Recepción de correo fallido por cuenta de correo externa. 2.3. Recepción de correo exitoso por cuenta de correo externa. 2.4. Recepción de correo exitoso por cuenta de correo externa.

Ilustración 26: Caso de Pruebas de Servicios de Correo

Fuente: Creación adecuada buenas prácticas de prueba de software

Se realizó la prueba para los siguientes cargos con sus respectivos atributos de envío y recepción de correos.

			ATRIBUTOS DE CORREO		
			SALIDA EXTERNA	ENVIO INTERNO	ENVIÓ EXTERNO
Nombre Grupo	Tipo Grupo	Descripción de Nombre			
G_ROF_SIN	GRUPO UNIDAD	UNIDAD DE SEGURIDAD DE LA INFORMACION			
G_00000149	GRUPO CARGO	ANALISTA DE SEGURIDAD DE LA INFORMACION	Sí	5 MB	3 MB
G_00000651	GRUPO CARGO	ANALISTA SENIOR DE SEGURIDAD DE LA INFORMACION	Sí	5 MB	3 MB
G_00000832	GRUPO CARGO	SUBGERENTE DE SEGURIDAD DE LA INFORMACION	Sí	5 MB	3 MB
G_00000866	GRUPO CARGO	PRACTICANTE DE SEGURIDAD DE LA INFORMACION	No	5 MB	Restringido

Ilustración 27: Cargos de Seguridad de la Información Mibanco 2015

Fuente: Basada en la Matriz Integral AD-Mibanco

5.3.2 Resultados obtenidos

Se obtuvieron los siguientes resultados:

- Se usó como muestra 4 usuarios y se realizaron 16 pruebas, no se encontraron observaciones, todas cumplieron con la restricción de envío y recepción.

				Casos de Prueba			
N°de Usuarios	Cuenta de Correo de Prueba Outlook	Cargo de Usuaio	Nombre Grupo	Envío y recepción Interno >= 5 MB	Envío y recepción Interno < 5 MB	Envío y recepción Externo >= 3 MB	Envío y recepción Externo < 3 MB
-	-	UNIDAD DE SEGURIDAD DE LA INFORMACION	G_ROF_SIN	-	-	-	-
1	carlos.soto.l@mibanco.com.pe	SUBGERENTE DE SEGURIDAD DE LA INFORMACION	G_00000832	✓	☒	✓	☒
3	huber.llanca.m@mibanco.com.pe	ANALISTA SENIOR DE SEGURIDAD DE LA INFORMACION	G_00000651	✓	☒	✓	☒
2	sandra.medina.a@mibanco.com.pe	ANALISTA DE SEGURIDAD DE LA INFORMACION	G_00000149	✓	☒	✓	☒
1	tania.maldonado.t@mibanco.com.pe	PRACTICANTE DE SEGURIDAD DE LA INFORMACION	G_00000866	✓	☒	☒	☒

Fallido	☒
Exitoso	✓

Ilustración 28: Resultados del Caso de Pruebas 1

Fuente: Creación adecuada buenas prácticas de prueba de software

5.4 ANÁLISIS DE LOS RESULTADOS

1. No se encontraron observaciones en las 16 pruebas realizadas de envíos y recepción de correos, pero es necesario indicar que la muestra fue muy acotada solo fueron 4 usuarios de prueba.
2. Para el caso del Practicante de Seguridad de la Información que tiene la salida de correo externo restringida como se observa en la ilustración 28, no hubo necesidad de realizar pruebas para el caso de envío y recepción a externos.
3. Es necesario indicar que esta prueba de envíos y recepción a correos es solo una referencia de todos los servicios que se podrían probar como: los niveles de Internet, los directorios compartidos y accesos a dispositivos de almacenamiento.

Capítulo 6: IMPLEMENTACIÓN EN ACTIVE DIRECTORY DE WINDOWS SERVER 2012

6.1 DESARROLLO DE LA IMPLEMENTACIÓN EN ACTIVE DIRECTORY DE WINDOWS SERVER 2012

6.1.1 Creación de Estructura de Grupos de Seguridad en Active Directory de Windows Server 2012:

En esta etapa de la Implementación se creará la estructura de grupos de Seguridad tomando como input el **ANEXO 2**.

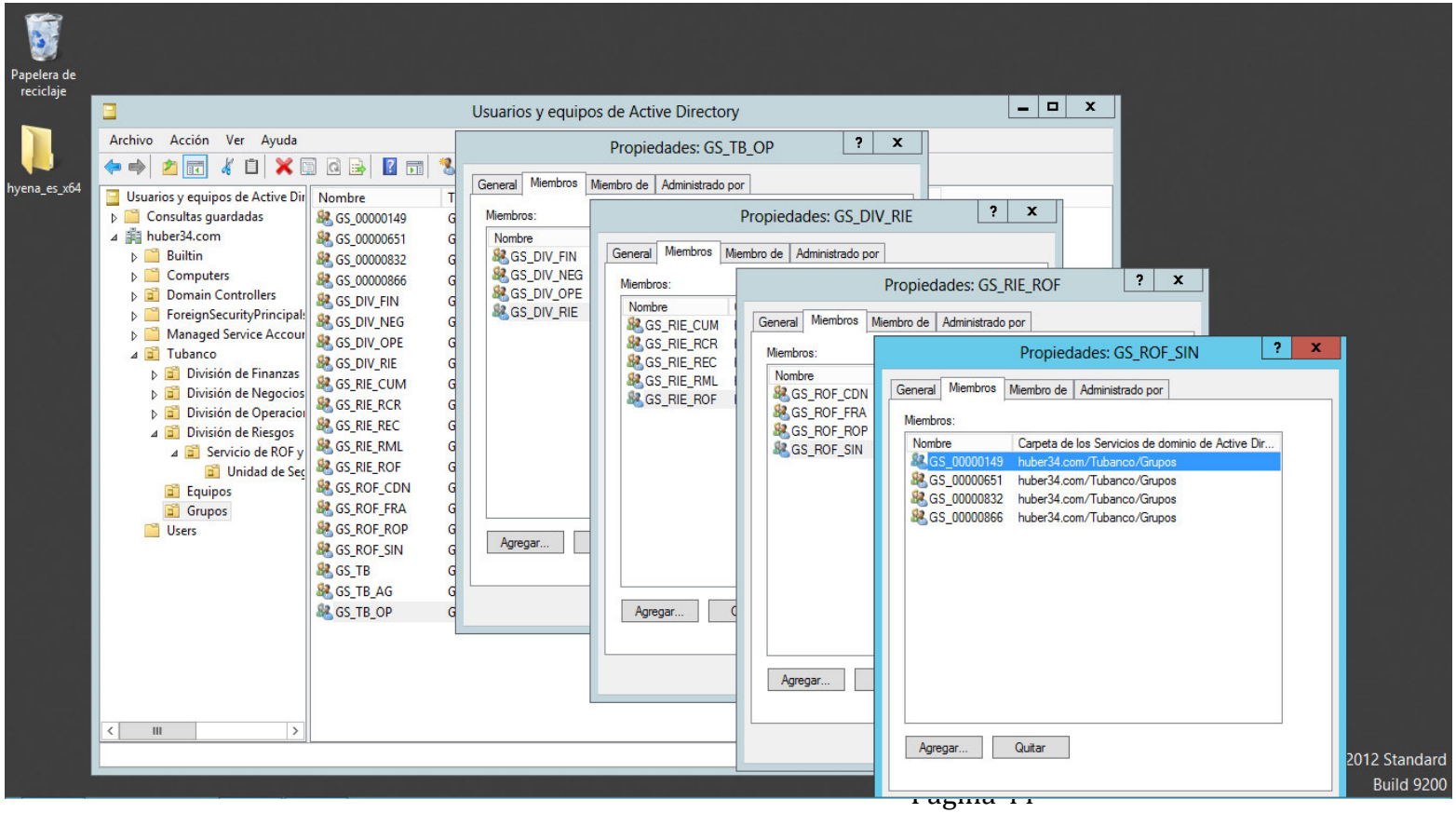


Ilustración 29: Creación de Grupos de Seguridad en AD

Fuente: Creación Propia

6.1.2 Creación de Políticas de Seguridad asociadas a Servicios de TI en Active Directory de Windows Server 2012:

En esta etapa de la Implementación se realizan todas las configuraciones en las directivas de seguridad de Active Directory (GPOs) asociadas a los servicios de TI como Correos, Internet, puertos USB y Directorios Compartidos, se tiene como input el **ANEXO 3**.

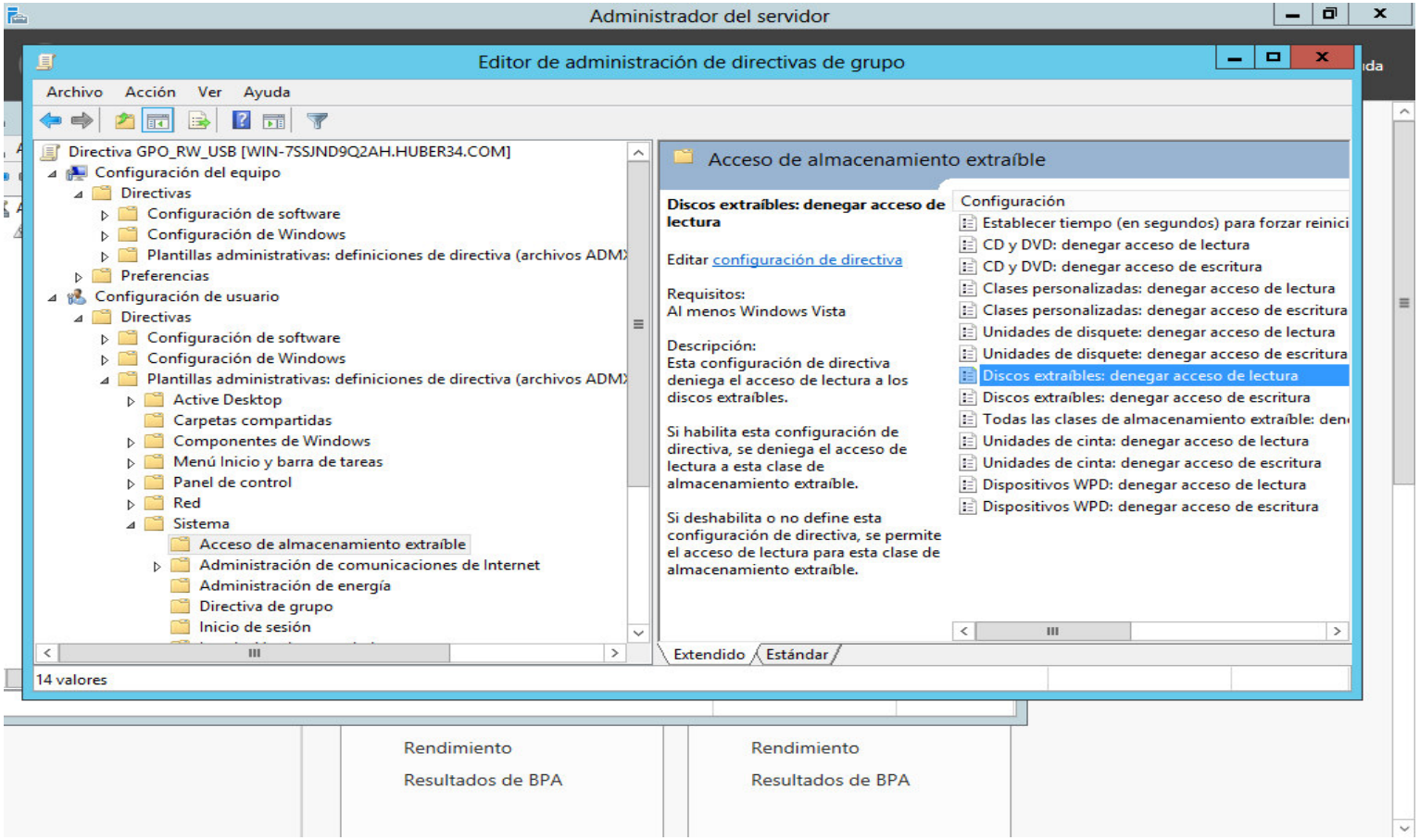


Ilustración 30: Configuración de Directivas en AD

Fuente: Creación Propia

6.1.3 Integración Grupos de Seguridad vs Servicios de TI:

En esta etapa de la implementación se integró los grupos de la estructura organizativa con los Servicios de TI, cabe señalar que los servicios de TI en Active Directory también son representan por grupos de Seguridad, se tiene como input el **ANEXO 3**.

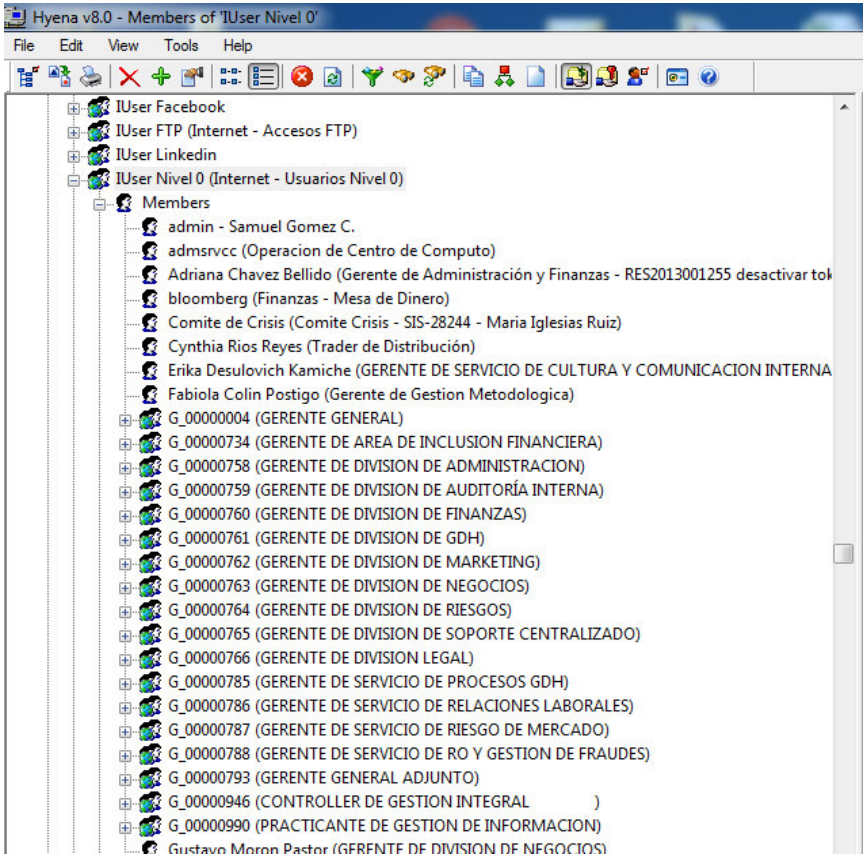


Ilustración 31: Integración de Grupos de Seguridad con Grupos de Servicios

Fuente: Creación Propia-Mibanco

6.1.4 Asignación de Usuarios a Grupos de Seguridad

En esta etapa de la Implementación se realizó la carga de los usuarios a los grupos de seguridad según el cargo que poseen, tomando como input el **ANEXO 2**.

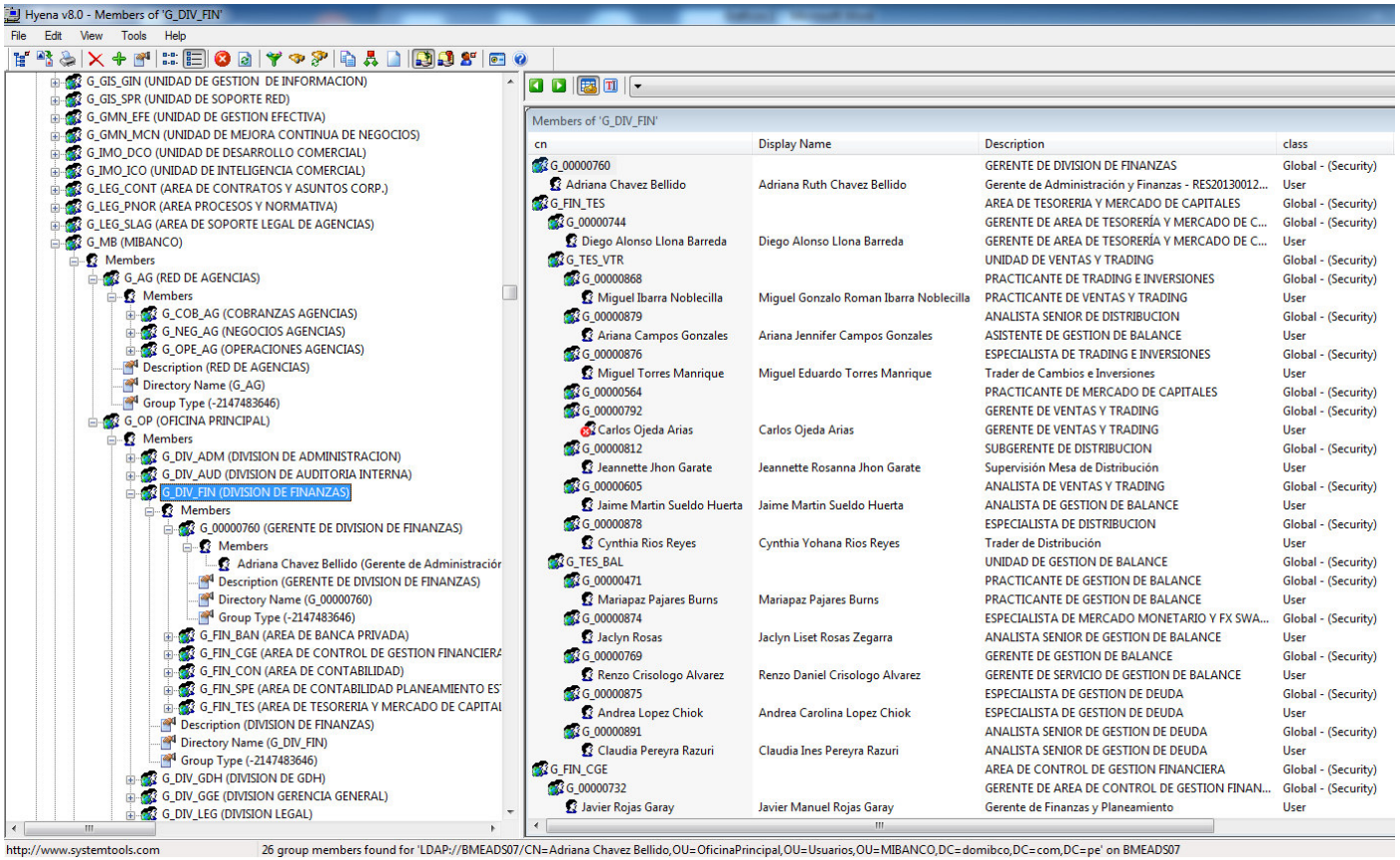
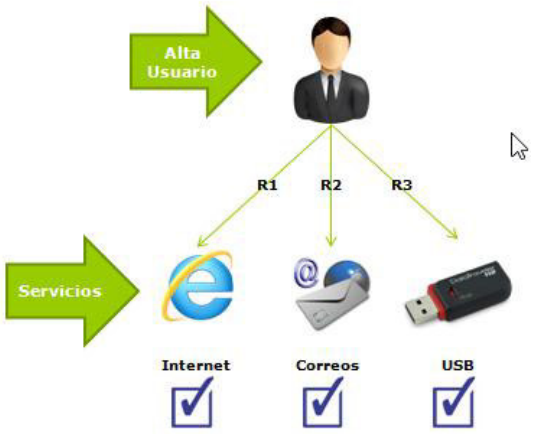
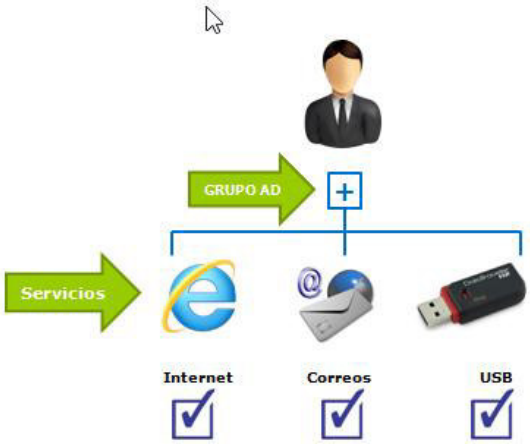


Ilustración 32: Asignación de Usuarios a Grupos de Seguridad

Fuente: Creación Propia-Mibanco

6.2 ANÁLISIS EN LA DE ATENCIÓN DE ACCESOS Y PERFILES LUEGO DE LA IMPLEMENTACIÓN

Teniendo en cuenta que se integraron solo 3 recursos como son: correo electrónico, dispositivo de almacenamiento y niveles de internet, además el SLA (acuerdo de nivel de servicio) para cada uno de estos requerimientos es de 4hras, se puede identificar las mejoras en el siguiente cuadro comparativo:

Antes de la Implementación	**Después de la Implementación:**
Los accesos se otorgan por usuario, para atender estos 3 requerimientos tomaría un tiempo de atención promedio que vendría a ser la sumatoria de lo tiempos de los requerimientos: R1+R2+R3=12hrs. 	Los accesos se otorgan por grupo, al asignar el usuario al grupo de seguridad este hereda accesos, entonces para atender estos 3 requerimientos tomaría un tiempo de atención promedio que vendría a ser equivalente al tiempo de cada uno de los requerimientos: R1=R2=R3=Rgs=4hrs. 

Como se puede apreciar el tiempo de atención de estos 3 requerimientos se reduce a 4 hras que representa el 33,3% del tiempo total de atención (12hras).

Análisis de la Atención en la Mesa de Ayuda

La siguiente Información fue tomada el 18/01/2016 del Aplicativo Mesa de Ayuda de la Entidad Bancaria (implementada en el mes de Mayo 2015), se toma como referencia este proyecto Accesos y Perfiles por las solicitudes de accesos de altas colaboradores, cabe señalar que dentro del mismo proyecto existe otros requerimientos lo cual hace referencial los cuadros, se puede observar que a partir del mes de Julio se cierran más tickets de atención, teniendo que en cuenta que esta implementación se realizó de manera parcial (3 servicios integrados) en el mes de Mayo del 2015 se observan mejoras de atención, a medida que se integren más servicios a AD estos números de atención deberían mejorar.

Período	Creados	Resuelta
January 2015	0	0
February 2015	0	0
March 2015	1311	919
April 2015	2277	2049
May 2015	2766	2610
June 2015	2849	2708
July 2015	2641	2808
August 2015	3067	3167
September 2015	2908	2937
October 2015	3069	3143
November 2015	3213	3171
December 2015	3066	3004
January 2016	2117	1886

Ilustración 33: Atención de Requerimientos Creados vs Atendidos de Accesos y Perfiles 2015

Fuente: Aplicativo Mesa de Ayuda de Mibanco

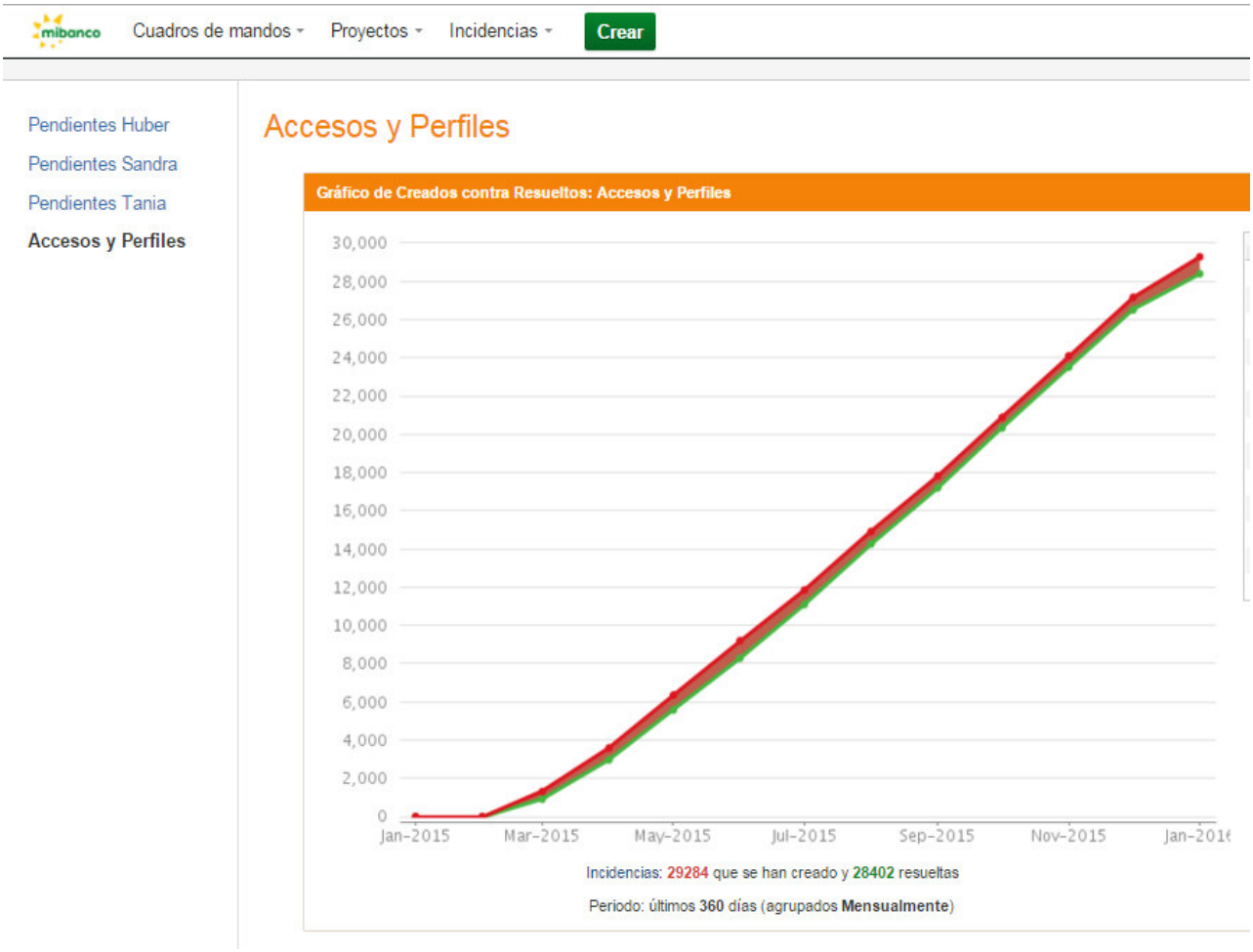


Ilustración 34:: Gráfico de Ticket Creados vs Atendidos de Accesos y Perfiles 2015

Fuente: Aplicativo Mesa de Ayuda de Mibanco

Capítulo 7: CONCLUSIONES Y RECOMENDACIONES

7.1 CONCLUSIONES

De acuerdo al planteamiento de la solución para el problema de la organización se concluye con lo siguiente:

- La integración de accesos de los recursos integrados por medio de grupos de seguridad minimizó el tiempo de atención de 12hras a 4hras, esto representa en una mejora del 66.6 % del tiempo, respecto del tiempo inicial empleado, para la atención de los 3 recursos integrados como son: correo electrónico, dispositivo de almacenamiento y niveles de internet.
- Es fundamental establecer una estructura de accesos y perfiles que esté basada en la estructura organizativa de una empresa, pues nos asegura una correcta segregación de accesos a recursos de TI según los niveles de jerarquía y funciones en la organización, esto se evidencia en el **ANEXO 2: Estructura de Grupos de Seguridad del Banco.**
- Establecer una estructura organizada de matrices de perfiles y roles en Directorio Activo otorga trazabilidad a las actividades de monitoreo de accesos, pues en el se puede conocer todos los accesos a los recursos del Directorio Activo que posee un colaborador de la empresa conociendo únicamente su cargo, esto se evidencia en el **ANEXO 3: Estructura Integral de Grupos AD vs Servicios de TI .**
- Una estructura organizada de accesos y perfiles mejora el cumplimiento del control de la Circular G-140-2009 "5.1) Seguridad Lógica; *a) Procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios"* y también los criterios de la seguridad de la información: confidencialidad, integridad y disponibilidad, centrándose en este último ya que los recursos se otorgan en el momento que el usuario lo necesita.

7.2 RECOMENDACIONES PARA FUTURAS INVESTIGACIONES

- Evaluar el grado de integración con la estructura de grupos de seguridad de Directorio Activo de todo software a adquirir, pues esto ayudaría a minimizar recursos en la implementación de las aplicaciones.
- Posterior a la implementación de la solución del presente trabajo, se debería mantener el concepto de Single Sign-On (SSO) que permite acceder a varias aplicaciones con una sola identificación.
- Se recomienda el uso de matrices de perfiles por cargos para tener registrado todos los accesos asignados a los recursos del Directorio Activo, además de ello es necesario llevar un control de cambios de todas las actualizaciones.

7.3 ANEXOS

ANEXO 1: Estructura Organizativa del Banco (División de Riesgos)

CODIGO	CARGO	DIVISION	AREA	SERVICIO	GERENCIA	SUBGERENCIA	UNIDAD	CODIGO REPORT
00000571	ANALISTA DE COBEX, CASTIGOS Y REFINANCIADOS	RIESGOS	RECUPERACIONES	RECUPERACIONES	ESTRATEGIA DE CO	ESTRATEGIA DE COBRA	COBEX, CASTIGOS Y F	00000839
00000839	SUPERVISOR DE COBEX, CASTIGOS Y REFINANCIADOS	RIESGOS	RECUPERACIONES	RECUPERACIONES	ESTRATEGIA DE CO	ESTRATEGIA DE COBRA	COBEX, CASTIGOS Y F	00000767
00000857	NORMALIZADOR DE CREDITOS Y CASTIGOS	RIESGOS	RECUPERACIONES	RECUPERACIONES	ESTRATEGIA DE CO	ESTRATEGIA DE COBRA	COBEX, CASTIGOS Y F	00000839
00000846	SUPERVISOR DE VENTA DE CARTERA Y JUDICIAL	RIESGOS	RECUPERACIONES	RECUPERACIONES	ESTRATEGIA DE CO	ESTRATEGIA DE COBRA	VENTA DE CARTERA	00000767
00000604	ANALISTA DE VENTA DE CARTERA Y JUDICIAL	RIESGOS	RECUPERACIONES	RECUPERACIONES	ESTRATEGIA DE CO	ESTRATEGIA DE COBRA	VENTA DE CARTERA	00000846
00000511	ABOGADO JUDICIAL	RIESGOS	RECUPERACIONES	RECUPERACIONES	ESTRATEGIA DE CO	ESTRATEGIA DE COBRA	VENTA DE CARTERA	00000846
00000696	ESPECIALISTA DE ESTRATEGIA DE RECUPERACIONES	RIESGOS	RECUPERACIONES	RECUPERACIONES	ESTRATEGIA DE CO	-	-	00000767
00000767	GERENTE DE ESTRATEGIA RECUPERACIONES	RIESGOS	RECUPERACIONES	RECUPERACIONES	ESTRATEGIA DE CO	-	-	00000741
00000578	ANALISTA DE ESTADISTICA DE RECUPERACIONES	RIESGOS	RECUPERACIONES	RECUPERACIONES	RECUPERACIONES	ESTADISTICA DE RECUP	-	00000813
00000626	ANALISTA SENIOR DE ESTADISTICA DE RECUPERACIONES	RIESGOS	RECUPERACIONES	RECUPERACIONES	RECUPERACIONES	ESTADISTICA DE RECUP	-	00000813
00000813	SUBGERENTE DE ESTADISTICA DE RECUPERACIONES	RIESGOS	RECUPERACIONES	RECUPERACIONES	RECUPERACIONES	ESTADISTICA DE RECUP	-	00000741
00000854	SUPERVISOR REGIONAL DE RECUPERACIONES	RIESGOS	RECUPERACIONES	RECUPERACIONES	TERRITORIAL REC	REGIONAL DE RECUPERA	-	00000791
00000791	GERENTE TERRITORIAL DE RECUPERACIONES	RIESGOS	RECUPERACIONES	RECUPERACIONES	TERRITORIAL REC	-	-	00000741
00000741	GERENTE DE AREA DE RECUPERACIONES	RIESGOS	RECUPERACIONES	-	-	-	-	00000764
00000689	ESPECIALISTA DE CONTROL DE GESTION DE RECUPERACIONES	RIESGOS	RECUPERACIONES	-	-	-	-	00000741
00000942	ANALISTA DE ESTRATEGIA DE RECUPERACIONES	RIESGOS	RECUPERACIONES	RECUPERACIONES	ESTRATEGIA DE CO	-	-	00000767
00000943	ANALISTA SENIOR DE ESTRATEGIA DE RECUPERACIONES	RIESGOS	RECUPERACIONES	RECUPERACIONES	ESTRATEGIA DE CO	-	-	00000767
00000858	EJECUTIVO DE RECUPERACIONES I	RIESGOS	RECUPERACIONES	RECUPERACIONES	TERRITORIAL REC	REGIONAL DE RECUPERA	-	00000528
00000859	EJECUTIVO DE RECUPERACIONES II	RIESGOS	RECUPERACIONES	RECUPERACIONES	TERRITORIAL REC	REGIONAL DE RECUPERA	-	00000528
00000860	EJECUTIVO DE RECUPERACIONES III	RIESGOS	RECUPERACIONES	RECUPERACIONES	TERRITORIAL REC	REGIONAL DE RECUPERA	-	00000528
00000742	GERENTE DE AREA DE RIESGO DE CREDITO	RIESGOS	RIESGO DE CREDITO	-	-	-	-	00000764
00000606	ANALISTA SENIOR DE ADMISION DE RIESGOS	RIESGOS	RIESGO DE CREDITO	RIESGO DE CREDITO	RIESGO DE CREDIT	ADMISION DE RIESGOS	-	00000796
00000861	ANALISTA DE ADMISION DE RIESGOS	RIESGOS	RIESGO DE CREDITO	RIESGO DE CREDITO	RIESGO DE CREDIT	ADMISION DE RIESGOS	-	00000796
00000796	SUBGERENTE DE ADMISION DE RIESGOS	RIESGOS	RIESGO DE CREDITO	RIESGO DE CREDITO	RIESGO DE CREDIT	ADMISION DE RIESGOS	-	00000742
00000631	ANALISTA SENIOR DE INFORMACION Y MODELOS	RIESGOS	RIESGO DE CREDITO	RIESGO DE CREDITO	INFORMACION Y M	-	-	00000816
00000816	GERENTE DE INFORMACION Y MODELOS	RIESGOS	RIESGO DE CREDITO	RIESGO DE CREDITO	INFORMACION Y M	-	-	00000742
00000584	ANALISTA DE INFORMACION Y MODELOS	RIESGOS	RIESGO DE CREDITO	RIESGO DE CREDITO	INFORMACION Y M	-	-	00000816
00000772	GERENTE DE GESTION Y SEGUIMIENTO	RIESGOS	RIESGO DE CREDITO	RIESGO DE CREDITO	GESTION Y SEGUIM	-	-	00000742
00000630	ANALISTA SENIOR DE GESTION Y SEGUIMIENTO	RIESGOS	RIESGO DE CREDITO	RIESGO DE CREDITO	GESTION Y SEGUIM	-	-	00000772
00000701	ESPECIALISTA DE GESTION Y SEGUIMIENTO	RIESGOS	RIESGO DE CREDITO	RIESGO DE CREDITO	GESTION Y SEGUIM	-	-	00000772
00000913	ANALISTA SENIOR DE SUPERVISION Y CONTRALORIA DE RIESGOS	RIESGOS	RIESGO DE CREDITO	RIESGO DE CREDITO	SUPERVISION Y CO	-	-	00000912
00000912	GERENTE DE SUPERVISION Y CONTRALORIA DE RIESGOS	RIESGOS	RIESGO DE CREDITO	RIESGO DE CREDITO	SUPERVISION Y CO	-	-	00000742
00000914	ANALISTA DE SUPERVISION Y CONTRALORIA DE RIESGOS	RIESGOS	RIESGO DE CREDITO	RIESGO DE CREDITO	SUPERVISION Y CO	-	-	00000912
00001005	ESPECIALISTA DE ADMISION DE RIESGOS	RIESGOS	RIESGO DE CREDITO	RIESGO DE CREDITO	RIESGO DE CREDIT	ADMISION DE RIESGOS	-	00000796
00000582	ANALISTA DE GESTION Y SEGUIMIENTO	RIESGOS	RIESGO DE CREDITO	RIESGO DE CREDITO	GESTION Y SEGUIM	-	-	00000772

CODIGO	CARGO	DIVISION	AREA	SERVICIO	GERENCIA	SUBGERENCIA	UNIDAD	CODIGO REPORT
00000787	GERENTE DE SERVICIO DE RIESGO DE MERCADO	RIESGOS	RIESGOS	RIESGO DE MERCADO	-	-	-	00000764
00000718	ESPECIALISTA DE RIESGO DE MERCADO	RIESGOS	RIESGOS	RIESGO DE MERCADO	-	-	-	00000787
00000595	ANALISTA DE RIESGO DE MERCADO	RIESGOS	RIESGOS	RIESGO DE MERCADO	-	-	-	00000787
00000618	ANALISTA SENIOR DE CONTINUIDAD DEL NEGOCIO	RIESGOS	RIESGOS	RIESGO OPERATIVO Y GES	RIESGO OPERATIV	CONTINUIDAD DEL NEG	-	00000807
00000807	SUBGERENTE DE CONTINUIDAD DEL NEGOCIO	RIESGOS	RIESGOS	RIESGO OPERATIVO Y GES	RIESGO OPERATIV	CONTINUIDAD DEL NEG	-	00000788
00000318	ANALISTA DE CONTINUIDAD DEL NEGOCIO	RIESGOS	RIESGOS	RIESGO OPERATIVO Y GES	RIESGO OPERATIV	CONTINUIDAD DEL NEG	-	00000807
00010131	ANALISTA DE CUMPLIMIENTO	RIESGOS	RIESGOS	RIESGOS	RIESGOS	CUMPLIMIENTO	-	00000810
00000590	ANALISTA DE PREVENCION DE FRAUDES	RIESGOS	RIESGOS	RIESGO OPERATIVO Y GES	RIESGO OPERATIV	PREVENCION DE FRAUDI	-	00000827
00000827	SUBGERENTE DE PREVENCION DE FRAUDES	RIESGOS	RIESGOS	RIESGO OPERATIVO Y GES	RIESGO OPERATIV	PREVENCION DE FRAUDI	-	00000788
00000650	ANALISTA SENIOR DE RIESGO OPERATIVO	RIESGOS	RIESGOS	RIESGO OPERATIVO Y GES	RIESGO OPERATIV	RIESGO OPERATIVO	-	00000831
00000831	SUBGERENTE DE RIESGO OPERATIVO	RIESGOS	RIESGOS	RIESGO OPERATIVO Y GES	RIESGO OPERATIV	RIESGO OPERATIVO	-	00000788
00000596	ANALISTA DE RIESGO OPERATIVO	RIESGOS	RIESGOS	RIESGO OPERATIVO Y GES	RIESGO OPERATIV	RIESGO OPERATIVO	-	00000831
00000651	ANALISTA SENIOR DE SEGURIDAD DE LA INFORMACION	RIESGOS	RIESGOS	RIESGO OPERATIVO Y GES	RIESGO OPERATIV	SEGURIDAD DE LA INFOI	-	00000832
00000832	SUBGERENTE DE SEGURIDAD DE LA INFORMACION	RIESGOS	RIESGOS	RIESGO OPERATIVO Y GES	RIESGO OPERATIV	SEGURIDAD DE LA INFOI	-	00000788
00000149	ANALISTA DE SEGURIDAD DE LA INFORMACION	RIESGOS	RIESGOS	RIESGO OPERATIVO Y GES	RIESGO OPERATIV	SEGURIDAD DE LA INFOI	-	00000832
00000788	GERENTE DE SERVICIO DE RO Y GESTION DE FRAUDES	RIESGOS	RIESGOS	RIESGO OPERATIVO Y GES	-	-	-	00000764
00000888	ESPECIALISTA OAU	RIESGOS	RIESGOS	RIESGOS	RIESGOS	CUMPLIMIENTO	-	00000810
00000720	ESPECIALISTA DE SEGURIDAD Y SALUD EN EL TRABAJO	RIESGOS	RIESGOS	RIESGOS	RIESGOS	CUMPLIMIENTO	-	00000810
00000711	ESPECIALISTA DE PLAFT	RIESGOS	RIESGOS	RIESGOS	RIESGOS	CUMPLIMIENTO	-	00000810
00000927	ANALISTA DE CUMPLIMIENTO PLAFT	RIESGOS	RIESGOS	RIESGOS	RIESGOS	CUMPLIMIENTO	-	00000810
00000889	ANALISTA OAU	RIESGOS	RIESGOS	RIESGOS	RIESGOS	CUMPLIMIENTO	-	00000810
00000810	SUBGERENTE DE CUMPLIMIENTO	RIESGOS	RIESGOS	RIESGOS	RIESGOS	CUMPLIMIENTO	-	00000764
00000694	ESPECIALISTA DE CUMPLIMIENTO NORMATIVO	RIESGOS	RIESGOS	RIESGOS	RIESGOS	CUMPLIMIENTO	-	00000810

ANEXO 2: Estructura de Grupos de Seguridad del Banco (División de Riesgos)

Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5	Nivel 6	Nombre Grupo	Tipo Grupo	Descripción de Nombre
G_MB	G_OP	G_DIV_RIE				G_DIV_RIE	GRUPO DIVISION	DIVISION DE RIESGOS
G_MB	G_OP	G_DIV_RIE	G_00000764			G_00000764	GRUPO CARGO	GERENTE DE DIVISION DE RIESGOS
G_MB	G_OP	G_DIV_RIE	G_RIE_CUM			G_RIE_CUM	GRUPO UNIDAD	AREA DE CUMPLIMIENTO
G_MB	G_OP	G_DIV_RIE	G_RIE_CUM	G_00000624		G_00000624	GRUPO CARGO	ANALISTA SENIOR DE CUMPLIMIENTO
G_MB	G_OP	G_DIV_RIE	G_RIE_CUM	G_00000927		G_00000927	GRUPO CARGO	ANALISTA DE CUMPLIMIENTO PLAFT
G_MB	G_OP	G_DIV_RIE	G_RIE_CUM	G_00010131		G_00010131	GRUPO CARGO	ANALISTA DE CUMPLIMIENTO
G_MB	G_OP	G_DIV_RIE	G_RIE_CUM	G_00000720		G_00000720	GRUPO CARGO	ESPECIALISTA DE SEGURIDAD Y SALUD EN EL TRABAJO
G_MB	G_OP	G_DIV_RIE	G_RIE_CUM	G_00000810		G_00000810	GRUPO CARGO	SUBGERENTE DE CUMPLIMIENTO
G_MB	G_OP	G_DIV_RIE	G_RIE_CUM	G_00000711		G_00000711	GRUPO CARGO	ESPECIALISTA DE PLAFT
G_MB	G_OP	G_DIV_RIE	G_RIE_CUM	G_00000694		G_00000694	GRUPO CARGO	ESPECIALISTA DE CUMPLIMIENTO NORMATIVO
G_MB	G_OP	G_DIV_RIE	G_RIE_CUM	G_00000888		G_00000888	GRUPO CARGO	ESPECIALISTA OAU
G_MB	G_OP	G_DIV_RIE	G_RIE_CUM	G_00000889		G_00000889	GRUPO CARGO	ANALISTA OAU
G_MB	G_OP	G_DIV_RIE	G_RIE_ROF			G_RIE_ROF	GRUPO UNIDAD	SERVICIO DE RO Y GESTION DE FRAUDES
G_MB	G_OP	G_DIV_RIE	G_RIE_ROF	G_00000788		G_00000788	GRUPO CARGO	GERENTE DE SERVICIO DE RO Y GESTION DE FRAUDES
G_MB	G_OP	G_DIV_RIE	G_RIE_ROF	G_ROF_CDN		G_ROF_CDN	GRUPO UNIDAD	UNIDAD DE CONTINUIDAD DE NEGOCIO
G_MB	G_OP	G_DIV_RIE	G_RIE_ROF	G_ROF_CDN	G_00000618	G_00000618	GRUPO CARGO	ANALISTA SENIOR DE CONTINUIDAD DEL NEGOCIO
G_MB	G_OP	G_DIV_RIE	G_RIE_ROF	G_ROF_CDN	G_00000318	G_00000318	GRUPO CARGO	ANALISTA DE CONTINUIDAD DEL NEGOCIO
G_MB	G_OP	G_DIV_RIE	G_RIE_ROF	G_ROF_CDN	G_00000807	G_00000807	GRUPO CARGO	SUBGERENTE DE CONTINUIDAD DEL NEGOCIO
G_MB	G_OP	G_DIV_RIE	G_RIE_ROF	G_ROF_FRA		G_ROF_FRA	GRUPO UNIDAD	UNIDAD DE PREVENCION DE FRAUDES
G_MB	G_OP	G_DIV_RIE	G_RIE_ROF	G_ROF_FRA	G_00000590	G_00000590	GRUPO CARGO	ANALISTA DE PREVENCION DE FRAUDES
G_MB	G_OP	G_DIV_RIE	G_RIE_ROF	G_ROF_FRA	G_00000827	G_00000827	GRUPO CARGO	SUBGERENTE DE PREVENCION DE FRAUDES
G_MB	G_OP	G_DIV_RIE	G_RIE_ROF	G_ROF_ROP		G_ROF_ROP	GRUPO UNIDAD	UNIDAD DE RIESGO OPERATIVO
G_MB	G_OP	G_DIV_RIE	G_RIE_ROF	G_ROF_ROP	G_00000596	G_00000596	GRUPO CARGO	ANALISTA DE RIESGO OPERATIVO
G_MB	G_OP	G_DIV_RIE	G_RIE_ROF	G_ROF_ROP	G_00000650	G_00000650	GRUPO CARGO	ANALISTA SENIOR DE RIESGO OPERATIVO
G_MB	G_OP	G_DIV_RIE	G_RIE_ROF	G_ROF_ROP	G_00000831	G_00000831	GRUPO CARGO	SUBGERENTE DE RIESGO OPERATIVO
G_MB	G_OP	G_DIV_RIE	G_RIE_ROF	G_ROF_SIN		G_ROF_SIN	GRUPO UNIDAD	UNIDAD DE SEGURIDAD DE LA INFORMACION
G_MB	G_OP	G_DIV_RIE	G_RIE_ROF	G_ROF_SIN	G_00000149	G_00000149	GRUPO CARGO	ANALISTA DE SEGURIDAD DE LA INFORMACION
G_MB	G_OP	G_DIV_RIE	G_RIE_ROF	G_ROF_SIN	G_00000651	G_00000651	GRUPO CARGO	ANALISTA SENIOR DE SEGURIDAD DE LA INFORMACION
G_MB	G_OP	G_DIV_RIE	G_RIE_ROF	G_ROF_SIN	G_00000832	G_00000832	GRUPO CARGO	SUBGERENTE DE SEGURIDAD DE LA INFORMACION
G_MB	G_OP	G_DIV_RIE	G_RIE_ROF	G_ROF_SIN	G_00000866	G_00000866	GRUPO CARGO	PRACTICANTE DE SEGURIDAD DE LA INFORMACION

Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5	Nivel 6	Nombre Grupo	Tipo Grupo	Descripción de Nombre
G_MB	G_OP	G_DIV_RIE				G_DIV_RIE	GRUPO DIVISION	DIVISION DE RIESGOS
G_MB	G_OP	G_DIV_RIE	G_RIE_RCR			G_RIE_RCR	GRUPO UNIDAD	AREA DE RIESGO DE CREDITO
G_MB	G_OP	G_DIV_RIE	G_RIE_RCR	G_00000742		G_00000742	GRUPO CARGO	GERENTE DE AREA DE RIESGO DE CREDITO
G_MB	G_OP	G_DIV_RIE	G_RIE_RCR	G_RCR_ADR		G_RCR_ADR	GRUPO UNIDAD	UNIDAD DE ADMISION DE RIESGOS
G_MB	G_OP	G_DIV_RIE	G_RIE_RCR	G_RCR_ADR	G_00000565	G_00000565	GRUPO CARGO	ANALISTA DE SUPERVISION Y CONTRALORIA DE CREDITO
G_MB	G_OP	G_DIV_RIE	G_RIE_RCR	G_RCR_ADR	G_00000861	G_00000861	GRUPO CARGO	ANALISTA DE ADMISION DE RIESGOS
G_MB	G_OP	G_DIV_RIE	G_RIE_RCR	G_RCR_ADR	G_00000606	G_00000606	GRUPO CARGO	ANALISTA SENIOR DE ADMISION DE RIESGOS
G_MB	G_OP	G_DIV_RIE	G_RIE_RCR	G_RCR_ADR	G_00000796	G_00000796	GRUPO CARGO	SUBGERENTE DE ADMISION DE RIESGOS
G_MB	G_OP	G_DIV_RIE	G_RIE_RCR	G_RCR_IMR		G_RCR_IMR	GRUPO UNIDAD	UNIDAD DE INFORMACION Y MODELOS
G_MB	G_OP	G_DIV_RIE	G_RIE_RCR	G_RCR_IMR	G_00000584	G_00000584	GRUPO CARGO	ANALISTA DE INFORMACION Y MODELOS
G_MB	G_OP	G_DIV_RIE	G_RIE_RCR	G_RCR_IMR	G_00000631	G_00000631	GRUPO CARGO	ANALISTA SENIOR DE INFORMACION Y MODELOS
G_MB	G_OP	G_DIV_RIE	G_RIE_RCR	G_RCR_IMR	G_00000816	G_00000816	GRUPO CARGO	GERENTE DE INFORMACION Y MODELOS
G_MB	G_OP	G_DIV_RIE	G_RIE_RCR	G_RCR_SEG		G_RCR_SEG	GRUPO UNIDAD	UNIDAD DE GESTION Y SEGUIMIENTO
G_MB	G_OP	G_DIV_RIE	G_RIE_RCR	G_RCR_SEG	G_00000582	G_00000582	GRUPO CARGO	ANALISTA DE GESTION Y SEGUIMIENTO
G_MB	G_OP	G_DIV_RIE	G_RIE_RCR	G_RCR_SEG	G_00000630	G_00000630	GRUPO CARGO	ANALISTA SENIOR DE GESTION Y SEGUIMIENTO
G_MB	G_OP	G_DIV_RIE	G_RIE_RCR	G_RCR_SEG	G_00000701	G_00000701	GRUPO CARGO	ESPECIALISTA DE GESTION Y SEGUIMIENTO
G_MB	G_OP	G_DIV_RIE	G_RIE_RCR	G_RCR_SEG	G_00000772	G_00000772	GRUPO CARGO	GERENTE DE GESTION Y SEGUIMIENTO
G_MB	G_OP	G_DIV_RIE	G_RIE_RCR	G_RCR_SUP		G_RCR_SUP	GRUPO UNIDAD	UNIDAD DE SUPERVISION DE RIESGOS
G_MB	G_OP	G_DIV_RIE	G_RIE_RCR	G_RCR_SUP	G_00000914	G_00000914	GRUPO CARGO	ANALISTA DE SUPERVISION Y CONTRALORIA DE RIESGOS
G_MB	G_OP	G_DIV_RIE	G_RIE_RCR	G_RCR_SUP	G_00000913	G_00000913	GRUPO CARGO	ANALISTA SENIOR DE SUPERVISION Y CONTRALORIA DE
G_MB	G_OP	G_DIV_RIE	G_RIE_RCR	G_RCR_SUP	G_00000912	G_00000912	GRUPO CARGO	GERENTE DE SUPERVISION Y CONTRALORIA DE RIESGOS
G_MB	G_OP	G_DIV_RIE	G_RIE_RML			G_RIE_RML	GRUPO UNIDAD	AREA DE RIESGOS DE MERCADO
G_MB	G_OP	G_DIV_RIE	G_00000595			G_00000595	GRUPO CARGO	ANALISTA DE RIESGO DE MERCADO
G_MB	G_OP	G_DIV_RIE	G_00000718			G_00000718	GRUPO CARGO	ESPECIALISTA DE RIESGO DE MERCADO
G_MB	G_OP	G_DIV_RIE	G_00000787			G_00000787	GRUPO CARGO	GERENTE DE SERVICIO DE RIESGO DE MERCADO

Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5	Nivel 6	Nombre Grupo	Tipo Grupo	Descripción de Nombre
G_MB	G_OP	G_DIV_RIE				G_DIV_RIE	GRUPO DIVISION	DIVISION DE RIESGOS
G_MB	G_OP	G_DIV_RIE	G_RIE_REC			G_RIE_REC	GRUPO UNIDAD	AREA DE RECUPERACIONES
G_MB	G_OP	G_DIV_RIE	G_RIE_REC	G_00000741		G_00000741	GRUPO CARGO	GERENTE DE AREA DE RECUPERACIONES
G_MB	G_OP	G_DIV_RIE	G_RIE_REC	G_REC_ESR		G_REC_ESR	GRUPO UNIDAD	UNIDAD DE ESTRATEGIA DE RECUPERACIONES
G_MB	G_OP	G_DIV_RIE	G_RIE_REC	G_REC_ESR	G_00000571	G_00000571	GRUPO CARGO	ANALISTA DE COBEX, CASTIGOS Y REFINANCIADOS
G_MB	G_OP	G_DIV_RIE	G_RIE_REC	G_REC_ESR	G_00000839	G_00000839	GRUPO CARGO	SUPERVISOR DE COBEX, CASTIGOS Y REFINANCIADOS
G_MB	G_OP	G_DIV_RIE	G_RIE_REC	G_REC_ESR	G_00000696	G_00000696	GRUPO CARGO	ESPECIALISTA DE ESTRATEGIA DE RECUPERACIONES
G_MB	G_OP	G_DIV_RIE	G_RIE_REC	G_REC_ESR	G_00000767	G_00000767	GRUPO CARGO	GERENTE DE ESTRATEGIA RECUPERACIONES
G_MB	G_OP	G_DIV_RIE	G_RIE_REC	G_REC_ESR	G_00000846	G_00000846	GRUPO CARGO	SUPERVISOR DE VENTA DE CARTERA Y JUDICIAL
G_MB	G_OP	G_DIV_RIE	G_RIE_REC	G_REC_ESR	G_00000604	G_00000604	GRUPO CARGO	ANALISTA DE VENTA DE CARTERA Y JUDICIAL
G_MB	G_OP	G_DIV_RIE	G_RIE_REC	G_REC_ESR	G_00000857	G_00000857	GRUPO CARGO	NORMALIZADOR DE CREDITOS Y CASTIGOS
G_MB	G_OP	G_DIV_RIE	G_RIE_REC	G_REC_ESR	G_00000942	G_00000942	GRUPO CARGO	ANALISTA DE ESTRATEGIA DE RECUPERACIONES
G_MB	G_OP	G_DIV_RIE	G_RIE_REC	G_REC_ESR	G_00000943	G_00000943	GRUPO CARGO	ANALISTA SENIOR DE ESTRATEGIA DE RECUPERACIONES
G_MB	G_OP	G_DIV_RIE	G_RIE_REC	G_REC_ESR	G_00000881	G_00000881	GRUPO CARGO	PRACTICANTE DE RECUPERACIONES
G_MB	G_OP	G_DIV_RIE	G_RIE_REC	G_REC_STR		G_REC_STR	GRUPO UNIDAD	UNIDAD DE ESTADISTICA DE RECUPERACIONES
G_MB	G_OP	G_DIV_RIE	G_RIE_REC	G_REC_STR	G_00000578	G_00000578	GRUPO CARGO	ANALISTA DE ESTADISTICA DE RECUPERACIONES
G_MB	G_OP	G_DIV_RIE	G_RIE_REC	G_REC_STR	G_00000626	G_00000626	GRUPO CARGO	ANALISTA SENIOR DE ESTADISTICA DE RECUPERACIONE
G_MB	G_OP	G_DIV_RIE	G_RIE_REC	G_REC_STR	G_00000689	G_00000689	GRUPO CARGO	ESPECIALISTA DE CONTROL DE GESTION DE RECUPERAC
G_MB	G_OP	G_DIV_RIE	G_RIE_REC	G_REC_STR	G_00000813	G_00000813	GRUPO CARGO	SUBGERENTE DE ESTADISTICA DE RECUPERACIONES
G_MB	G_OP	G_DIV_RIE	G_RIE_REC	G_REC_TER		G_REC_TER	GRUPO UNIDAD	UNIDAD TERRITORIAL DE RECUPERACIONES
G_MB	G_OP	G_DIV_RIE	G_RIE_REC	G_REC_TER	G_00000791	G_00000791	GRUPO CARGO	GERENTE DE TERRITORIAL RECUPERACIONES

ANEXO 3: Estructura Integral de Grupos AD vs Servicios de TI (División de Riesgos)

			INTERNET		ATRIBUTOS DE CORREO				DISP. USB	PERMISOS DE DIRECTORIOS COMPARTIDOS																															
Nombre Grupo	Descripción de Nombre	TIPO CARGO	NIVELES	WIRELESS	SALIDA EXTERNA	ALMACENAMIENTO	ENVIO INTERNO	ENVIÓ EXTERNO	NIVELES	PRIV_MIBANCO	PRIV_OFICINA PRINCIPAL	PRIV_DIV. ADMINISTRACION	PRIV_DIV. AUDITORIA INTERNA	PRIV_DIV. FINANZAS	PRIV_DIV. GDH	PRIV_DIV. GERENCIA GENERAL	PRIV_DIV. GERENCIA GENERAL ADJ	PRIV_DIV. LEGAL	PRIV_DIV. MARKETING	PRIV_DIV. NEGOCIOS	PRIV_DIV. RIESGOS	PRIV_DIV. SOPORTE CENTRALIZADO	COMP_MIBANCO	COMP_OFICINA PRINCIPAL	COMP_DIV. ADMINISTRACION	COMP_DIV. AUDITORIA INTERNA	COMP_DIV. FINANZAS	COMP_DIV. GDH	COMP_DIV. GERENCIA GENERAL	COMP_DIV. GERENCIA GENERAL ADJ	COMP_DIV. LEGAL	COMP_DIV. MARKETING	COMP_DIV. NEGOCIOS	COMP_DIV. RIESGOS	COMP_DIV. SOPORTE CENTRALIZADO
G_DIV_RIE	DIVISION DE RIESGOS	C																																				
G_00000764	GERENTE DE DIVISION DE RIESGOS	C	IUser Nivel 0	Sí	Sí	GRUPO AVANZADO	10 MB	5 MB	USB_BloqueoTotal																													
G_RIE_CUM	AREA DE CUMPLIMIENTO	C																																				
G_00000624	ANALISTA SENIOR DE CUMPLIMIENTO	C	Iuser Nivel 1	Sí	No	GRUPO D	5 MB	Restringido	USB_BloqueoTotal																														
G_00000327	ANALISTA DE CUMPLIMIENTO PLAFT	C	IUser Nivel 2	Sí					USB_BloqueoTotal																														
G_00010131	ANALISTA DE CUMPLIMIENTO	C	IUser Nivel 2	Sí	No	GRUPO D	5 MB	Restringido	USB_BloqueoTotal																														
G_00000720	ESPECIALISTA DE SEGURIDAD Y SALUD EN EL TRABAJO	C	IUser Nivel 1	Sí	Sí	GRUPO D	5 MB	3 MB	USB_BloqueoTotal																														
G_00000810	SUBGERENTE DE CUMPLIMIENTO	C	IUser Nivel 1	Sí	Sí	GRUPO C	5 MB	Restringido	USB_BloqueoTotal																														
G_00000711	ESPECIALISTA DE PLAFT	C	IUser Nivel 1	Sí	No	GRUPO D	5 MB	Restringido	USB_BloqueoTotal																														
G_00000694	ESPECIALISTA DE CUMPLIMIENTO NORMATIVO	C	IUser Nivel 1	Sí	No	GRUPO D	5 MB	Restringido	USB_BloqueoTotal																														
G_00000888	ESPECIALISTA OAU	C	IUser Nivel 1	Sí					USB_BloqueoTotal																														
G_00000889	ANALISTA OAU	C	IUser Nivel 1	Sí					USB_BloqueoTotal																														
G_RIE_RML	AREA DE RIESGOS DE MERCADO	C																																				
G_00000595	ANALISTA DE RIESGO DE MERCADO	C	IUser Nivel 2	Sí	Sí	GRUPO D	5 MB	3 MB	USB_BloqueoTotal																														
G_00000718	ESPECIALISTA DE RIESGO DE MERCADO	C	IUser Nivel 1	Sí	Sí	GRUPO D	5 MB	3 MB	USB_BloqueoTotal																														
G_00000787	GERENTE DE SERVICIO DE RIESGO DE MERCADO	C	IUser Nivel 0	Sí	Sí	GRUPO A	10 MB	3 MB	USB_BloqueoTotal																														

			INTERNET		ATRIBUTOS DE CORREO				DISP. USB	PERMISOS DE DIRECTORIOS COMPARTIDOS																										
Nombre Grupo	Descripción de Nombre	TIPO CARGO	NIVELES	WIRELESS	SALIDA EXTERNA	ALMACENAMIENTO	ENVIO INTERNO	ENVIÓ EXTERNO	NIVELES	PRIV_MIBANCO	PRIV_OFICINA PRINCIPAL	PRIV_DIV. ADMINISTRACION	PRIV_DIV. AUDITORIA INTERNA	PRIV_DIV. FINANZAS	PRIV_DIV. GDH	PRIV_DIV. GERENCIA GENERAL	PRIV_DIV. GERENCIA GENERAL ADJ	PRIV_DIV. LEGAL	PRIV_DIV. MARKETING	PRIV_DIV. NEGOCIOS	PRIV_DIV. RIESGOS	PRIV_DIV. SOPORTE CENTRALIZADO	COMP_MIBANCO	COMP_OFICINA PRINCIPAL	COMP_DIV. ADMINISTRACION	COMP_DIV. AUDITORIA INTERNA	COMP_DIV. FINANZAS	COMP_DIV. GDH	COMP_DIV. GERENCIA GENERAL	COMP_DIV. GERENCIA GENERAL ADJ	COMP_DIV. LEGAL	COMP_DIV. MARKETING	COMP_DIV. NEGOCIOS	COMP_DIV. RIESGOS	COMP_DIV. SOPORTE CENTRALIZADO
G_RIE_ROF	SERVICIO DE RO Y GESTION DE FRAUDES	C																																	
G_00000788	GERENTE DE SERVICIO DE RO Y GESTION DE FRAUDES	C	IUser Nivel 0	Sí	Sí	GRUPO A	10 MB	3 MB	USB_BloqueoTotal																										
G_ROF_CDN	UNIDAD DE CONTINUIDAD DE NEGOCIO	C																																	
G_00000618	ANALISTA SENIOR DE CONTINUIDAD DEL NEGOCIO	C	IUser Nivel 1	Sí	Sí	GRUPO D	5 MB	3 MB	USB_BloqueoTotal																										
G_00000318	ANALISTA DE CONTINUIDAD DEL NEGOCIO	C	IUser Nivel 2	Sí					USB_BloqueoTotal																										
G_00000807	SUBGERENTE DE CONTINUIDAD DEL NEGOCIO	C	IUser Nivel 1	Sí	Sí	GRUPO C	5 MB	3 MB	USB_BloqueoTotal																										
G_ROF_FRA	UNIDAD DE PREVENCION DE FRAUDES	C																																	
G_00000590	ANALISTA DE PREVENCION DE FRAUDES	C	IUser Nivel 2	Sí	No	GRUPO D	5 MB	Restringido	USB_BloqueoTotal																										
G_00000827	SUBGERENTE DE PREVENCION DE FRAUDES	C	IUser Nivel 1	Sí	Sí	GRUPO C	5 MB	Restringido	USB_BloqueoTotal																										
G_ROF_ROP	UNIDAD DE RIESGO OPERATIVO	C																																	
G_00000596	ANALISTA DE RIESGO OPERATIVO	C	IUser Nivel 2	Sí	Sí	GRUPO D	5 MB	3 MB	USB_BloqueoTotal																										
G_00000650	ANALISTA SENIOR DE RIESGO OPERATIVO	C	IUser Nivel 1	Sí	Sí	GRUPO D	5 MB	3 MB	USB_BloqueoTotal																										
G_00000831	SUBGERENTE DE RIESGO OPERATIVO	C	IUser Nivel 1	Sí	Sí	GRUPO C	5 MB	3 MB	USB_BloqueoTotal																										
G_ROF_SIN	UNIDAD DE SEGURIDAD DE LA INFORMACION	C																																	
G_00000149	ANALISTA DE SEGURIDAD DE LA INFORMACION	C	IUser Nivel 2	Sí	Sí	GRUPO D	5 MB	3 MB	USB_SoloLectura																										
G_00000651	ANALISTA SENIOR DE SEGURIDAD DE LA INFORMACION	C	IUser Nivel 1	Sí	Sí	GRUPO D	5 MB	3 MB	USB_SoloLectura																										
G_00000832	SUBGERENTE DE SEGURIDAD DE LA INFORMACION	C	IUser Nivel 1	Sí	Sí	GRUPO C	5 MB	3 MB	USB_SoloLectura																										
G_00000866	PRACTICANTE DE SEGURIDAD DE LA INFORMACION	P	IUser Nivel 2	No	No	GRUPO D	5 MB	Restringido	USB_BloqueoTotal																										

			INTERNET		ATRIBUTOS DE CORREO				DISP. USB	PERMISOS DE DIRECTORIOS COMPARTIDOS																															
Nombre Grupo	Descripción de Nombre	TIPO CARGO	NIVELES	WIRELESS	SALIDA EXTERNA	ALMACENAMIENTO	ENVIO INTERNO	ENVIÓ EXTERNO	NIVELES	PRIV_MIBANCO	PRIV_OFICINA PRINCIPAL	PRIV_DIV. ADMINISTRACION	PRIV_DIV. AUDITORIA INTERNA	PRIV_DIV. FINANZAS	PRIV_DIV. GDH	PRIV_DIV. GERENCIA GENERAL	PRIV_DIV. GERENCIA GENERAL ADJ	PRIV_DIV. LEGAL	PRIV_DIV. MARKETING	PRIV_DIV. NEGOCIOS	PRIV_DIV. RIESGOS	PRIV_DIV. SOPORTE CENTRALIZADO	COMP_MIBANCO	COMP_OFICINA PRINCIPAL	COMP_DIV. ADMINISTRACION	COMP_DIV. AUDITORIA INTERNA	COMP_DIV. FINANZAS	COMP_DIV. GDH	COMP_DIV. GERENCIA GENERAL	COMP_DIV. GERENCIA GENERAL ADJ	COMP_DIV. LEGAL	COMP_DIV. MARKETING	COMP_DIV. NEGOCIOS	COMP_DIV. RIESGOS	COMP_DIV. SOPORTE CENTRALIZADO
G_RIE_RCR	AREA DE RIESGO DE CREDITO	C																																				
G_00000742	GERENTE DE AREA DE RIESGO DE CREDITO	C	IUser Nivel 1	Sí	Sí	GRUPO A	10 MB	3 MB	USB_BloqueoTotal																													
G_RCR_ADR	UNIDAD DE ADMISION DE RIESGOS	C																																				
G_00000565	ANALISTA DE SUPERVISION Y CONTRALORIA DE CREDITOS	C	Iuser Nivel 1	Sí					USB_BloqueoTotal																														
G_00000861	ANALISTA DE ADMISION DE RIESGOS	C	IUser Nivel 2	Sí	Sí	GRUPO D	5 MB	3 MB	USB_BloqueoTotal																														
G_00000606	ANALISTA SENIOR DE ADMISION DE RIESGOS	C	IUser Nivel 1	Sí	Sí	GRUPO D	5 MB	3 MB	USB_BloqueoTotal																														
G_00000796	SUBGERENTE DE ADMISION DE RIESGOS	C	IUser Nivel 1	Sí	Sí	GRUPO C	5 MB	3 MB	USB_BloqueoTotal																														
G_RCR_IMR	UNIDAD DE INFORMACION Y MODELOS	C																																				
G_00000584	ANALISTA DE INFORMACION Y MODELOS	C	IUser Nivel 2	Sí	Sí	GRUPO D	5 MB	3 MB	USB_BloqueoTotal																														
G_00000631	ANALISTA SENIOR DE INFORMACION Y MODELOS	C	IUser Nivel 1	Sí	Sí	GRUPO D	5 MB	3 MB	USB_BloqueoTotal																														
G_00000816	GERENTE DE INFORMACION Y MODELOS	C	IUser Nivel 1	Sí	Sí	GRUPO C	5 MB	3 MB	USB_BloqueoTotal																														
G_RCR_SEG	UNIDAD DE GESTION Y SEGUIMIENTO	C																																				
G_00000582	ANALISTA DE GESTION Y SEGUIMIENTO	C	Iuser Nivel 1	Sí	Sí	GRUPO D	5 MB	3 MB	USB_BloqueoTotal																														
G_00000630	ANALISTA SENIOR DE GESTION Y SEGUIMIENTO	C	IUser Nivel 1	Sí	Sí	GRUPO D	5 MB	3 MB	USB_BloqueoTotal																														
G_00000701	ESPECIALISTA DE GESTION Y SEGUIMIENTO	C	IUser Nivel 1	Sí	Sí	GRUPO D	5 MB	3 MB	USB_BloqueoTotal																														
G_00000772	GERENTE DE GESTION Y SEGUIMIENTO	C	IUser Nivel 1	Sí	Sí	GRUPO C	5 MB	3 MB	USB_BloqueoTotal																														
G_RCR_SUP	UNIDAD DE SUPERVISION DE RIESGOS	C																																				
G_00000314	ANALISTA DE SUPERVISION Y CONTRALORIA DE RIESGOS	C	IUser Nivel 2	Sí					USB_BloqueoTotal																														
G_00000313	ANALISTA SENIOR DE SUPERVISION Y CONTRALORIA DE RIESGOS	C	IUser Nivel 1	Sí					USB_BloqueoTotal																														
G_00000312	GERENTE DE SUPERVISION Y CONTRALORIA DE RIESGOS	C	IUser Nivel 1	Sí					USB_BloqueoTotal																														

			INTERNET		ATRIBUTOS DE CORREO				DISP. USB	PERMISOS DE DIRECTORIOS COMPARTIDOS																									
Nombre Grupo	Descripción de Nombre	TIPO CARGO	NIVELES	WIRELESS	SALIDA EXTERNA	ALMACENAMIENTO	ENVIO INTERNO	ENVIÓ EXTERNO	NIVELES	PRIV_MIBANCO	PRIV_OFICINA PRINCIPAL	PRIV_DIV. ADMINISTRACION	PRIV_DIV. AUDITORIA INTERNA	PRIV_DIV. FINANZAS	PRIV_DIV. GDH	PRIV_DIV. GERENCIA GENERAL	PRIV_DIV. GERENCIA GENERAL ADJ	PRIV_DIV. LEGAL	PRIV_DIV. MARKETING	PRIV_DIV. NEGOCIOS	PRIV_DIV. RIESGOS	PRIV_DIV. SOPORTE CENTRALIZADO	COMP_MIBANCO	COMP_OFICINA PRINCIPAL	COMP_DIV. ADMINISTRACION	COMP_DIV. AUDITORIA INTERNA	COMP_DIV. FINANZAS	COMP_DIV. GDH	COMP_DIV. GERENCIA GENERAL	COMP_DIV. GERENCIA GENERAL ADJ	COMP_DIV. LEGAL	COMP_DIV. MARKETING	COMP_DIV. NEGOCIOS	COMP_DIV. RIESGOS	COMP_DIV. SOPORTE CENTRALIZADO
G_RIE_REC	AREA DE RECUPERACIONES	C																																	
G_00000741	GERENTE DE AREA DE RECUPERACIONES	C	IUser Nivel 1	Sí	Sí	GRUPO A	10 MB	3 MB	USB_BloqueoTotal																										
G_REC_ESR	UNIDAD DE ESTRATEGIA DE RECUPERACIONES	C																																	
G_00000571	ANALISTA DE COBEX, CASTIGOS Y REFINANCIADOS	C	IUser Nivel 2	Sí	No	GRUPO D	5 MB	Restringido	USB_BloqueoTotal																										
G_00000839	SUPERVISOR DE COBEX, CASTIGOS Y REFINANCIADOS	C	IUser Nivel 1	Sí	No	GRUPO C	5 MB	Restringido	USB_BloqueoTotal																										
G_00000696	ESPECIALISTA DE ESTRATEGIA DE RECUPERACIONES	C	IUser Nivel 1	Sí	Sí	GRUPO D	5 MB	3 MB	USB_BloqueoTotal																										
G_00000767	GERENTE DE ESTRATEGIA RECUPERACIONES	C	IUser Nivel 1	Sí	Sí	GRUPO C	5 MB	3 MB	USB_BloqueoTotal																										
G_00000846	SUPERVISOR DE VENTA DE CARTERA Y JUDICIAL	C	IUser Nivel 1	Sí	No	GRUPO C	5 MB	Restringido	USB_BloqueoTotal																										
G_00000604	ANALISTA DE VENTA DE CARTERA Y JUDICIAL	C	IUser Nivel 2	Sí	No	GRUPO D	5 MB	Restringido	USB_BloqueoTotal																										
G_00000857	NORMALIZADOR DE CREDITOS Y CASTIGOS	C	IUser Nivel 1	Sí	No	GRUPO D	5 MB	Restringido	USB_BloqueoTotal																										
G_00000942	ANALISTA DE ESTRATEGIA DE RECUPERACIONES	C		Sí					USB_BloqueoTotal																										
G_00000943	ANALISTA SENIOR DE ESTRATEGIA DE RECUPERACIONES	C		Sí					USB_BloqueoTotal																										
G_00000881	PRACTICANTE DE RECUPERACIONES	P	IUser Nivel 2	No	No	GRUPO D	5 MB	Restringido	USB_BloqueoTotal																										
G_REC_STR	UNIDAD DE ESTADISTICA DE RECUPERACIONES	C																																	
G_00000578	ANALISTA DE ESTADISTICA DE RECUPERACIONES	C	IUser Nivel 2	Sí	Sí	GRUPO D	5 MB	3 MB	USB_BloqueoTotal																										
G_00000626	ANALISTA SENIOR DE ESTADISTICA DE RECUPERACIONES	C	IUser Nivel 1	Sí	Sí	GRUPO D	5 MB	3 MB	USB_BloqueoTotal																										
G_00000689	ESPECIALISTA DE CONTROL DE GESTION DE RECUPERACIONES	C	IUser Nivel 1	Sí	Sí	GRUPO D	5 MB	3 MB	USB_BloqueoTotal																										
G_00000813	SUBGERENTE DE ESTADISTICA DE RECUPERACIONES	C	IUser Nivel 1	Sí	Sí	GRUPO C	5 MB	3 MB	USB_BloqueoTotal																										
G_REC_TER	UNIDAD TERRITORIAL DE RECUPERACIONES	C																																	
G_00000731	GERENTE DE TERRITORIAL RECUPERACIONES	C		Sí	Sí	GRUPO C	5 MB	3 MB	USB_BloqueoTotal																										

7.4 REFERENCIAS BIBLIOGRÁFICAS

LIBROS:

- BRIAN DESMOND, JOE RICHARDS, ROBBIE ALLEN Y ALISTAR G. LOWE NORRIS; "Active Directory 5th Edition"; Editorial: Orelly (2013); United States of America.

- CURT SIMMONS;"Active Directory Bible" Editorial: IDG Books Worldwide, Inc. (2001); United States of América.

- JESUS NIÑO CAMAZON; "Sistemas operativos en red" Editorial: Editex (2011); España.

- BRAHIM NEDJIMI, LOIC THOBOIS; "Preparación a la certificación MCSE Exchange Server 2013" Editorial: ENI (2014); Barcelona-España.

- ROGER S. PRESSMAN; "Ingeniería del Software un enfoque práctico-Séptima edición" Editorial: Mac Graw-Hill (2010); México.

NORMAS Y ESTANDARES

- CIRCULAR Nº G- 140 -2009; Superintendencia de Banca y Seguros (SBS).

- ESTÁNDAR INTERNACIONAL ISO/IEC 27001; Primera Edición 2005-10-15.

- NORMA TÉCNICA PERUANA "NTP-ISO/ IEC 17799:2007.

PROCEDIMIENTOS:

- MAN-RIE-101 MANUAL DE CONTROL DE ACCESOS; Entidad Financiera Mibanco.

PAPERS:

- RAFAEL CALZADA PRADA; " Introducción al Servicio de Directorios"
- Mª PILAR GONZÁLEZ FÉREZ; " Configuración de Active Directory"
- ANTONI MARTÍNEZ BALLESTE-JORDI CASTELLA ROCA; " Servicio de Directorio"
- ING. LÁZARO RAMOS - MSC. MIRIEL MARTÍN; " Implementación de un Servidor Samba con autenticación LDAP como alternativa Libre a los Servidores de Dominio Windows"

URLs:

- web.archive.org/web/http://es.tldp.org/Tutoriales/doc-openldap-samba-cups-python/htmls/openldap-que-es.html.
- http://itilv3.osiatis.es/operacion_servicios_TI/gestion_acceso_servicios_ti.php
- https://technet.microsoft.com/es-es/windowsserver/bb310732.aspx
- https://technet.microsoft.com/es-es/library/hh147307(v=ws.10).aspx
- https://msdn.microsoft.com/es-es/library/cc781446(v=ws.10).aspx
- https://docs.oracle.com/cd/E24842_01/html/E23286/docinfo.html#scrolltoc